P-791R v2

G.SHDSL.bis Router

User's Guide

Version 3.40
5/2007
Edition 2

DEFAULT LOGIN	
IP Address	http://192.168.1.1
Administrator Password	1234
User Password	user

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.

✍ It is recommended you use the web configurator to configure the ZyXEL Device.

- Supporting Disk

  Refer to the included CD for support documents.
- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

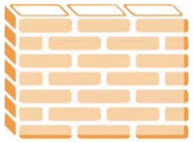
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The P-791R v2 may be referred to as the "ZyXEL Device", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance** > **Log** > **Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

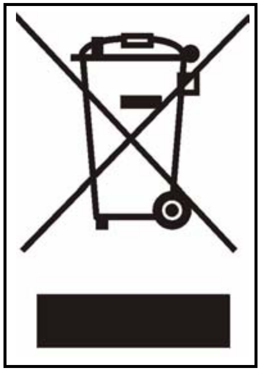
ZyXEL Device 	Computer 	Notebook computer
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- ONLY qualified service personnel should service or disassemble this device.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

This product is recyclable. Dispose of it properly.



Contents Overview

Table of Contents

Chapter 25

Chapter 26

Chapter 27

Chapter 28

Chapter 29

List of Figures

List of Tables

PART I

Introduction, Wizards and Tutorials

1

Getting To Know Your ZyXEL Device

This chapter introduces the main features and applications of your ZyXEL Device.

1.1 Overview

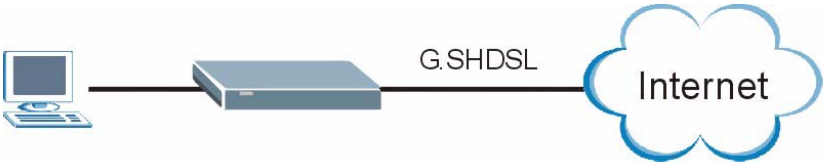
The ZyXEL Device is a G.SHDSL (G.992.1, Symmetrical high-speed Digital Subscriber Line).bis Router providing high-speed LAN-to-LAN connection and Internet access through G.SHDSL.bis connection over the telephone line. You can use your ZyXEL Device for either IP routing or bridging depending on your ISP (Internet Service Provider) configuration.

See Appendix A on page 281 for a complete list of features you can configure on your ZyXEL Device.

1.1.1 High-speed Internet Access

The ZyXEL Device is the ideal high-speed Internet access solution. In addition, unlike ADSL or VDSL, G.SHDSL.bis supports the same high speed for transmission and receiving.

Figure 1 High-speed Internet Access with Your ZyXEL Device



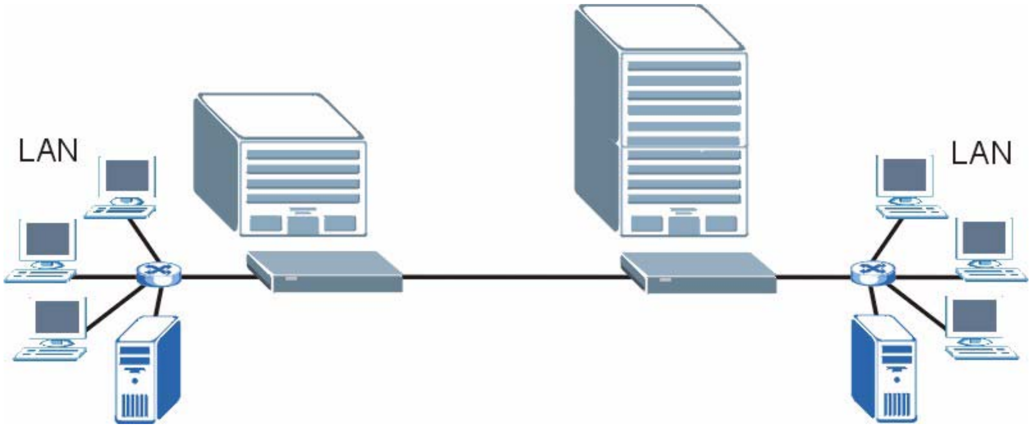
For Internet access, connect the DSL port to the phone port. Then, connect your computer or server to the ETHERNET port. (See the Quick Start Guide for detailed instructions about hardware connections.) Next, set up the ZyXEL Device as a router or as a bridge, depending on the desired configuration. As a router, the ZyXEL Device provides security and networking functionality. As a bridge, the ZyXEL Device minimizes the configuration changes you have to make in your existing network.

1.1.2 High-speed Point-to-point Connections

Use two ZyXEL Devices to create a cost-effective, high-speed connection for high-bandwidth applications such as videoconferencing and distance learning. The ZyXEL Devices provide a simple, fast point-to-point connection between two geographically-dispersed networks.

In the following example, two ZyXEL Devices connect the headquarters and a branch office.

Figure 2 Point-to-point Connections with Your ZyXEL Device



See Chapter 4 on page 55 for more information on setting up point-to-point connections.

1.2 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser. See Chapter 2 on page 37.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers. See Appendix G on page 325.
- SMT. System Management Terminal is a text-based configuration menu that you can use to configure your device. See Chapter 17 on page 163.
- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup/restore. See Chapter 11 on page 119.
- SNMP. The device can be monitored and/or managed by an SNMP manager. See Chapter 11 on page 119.

1.3 Good Habits for Managing the ZyXEL Device

Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

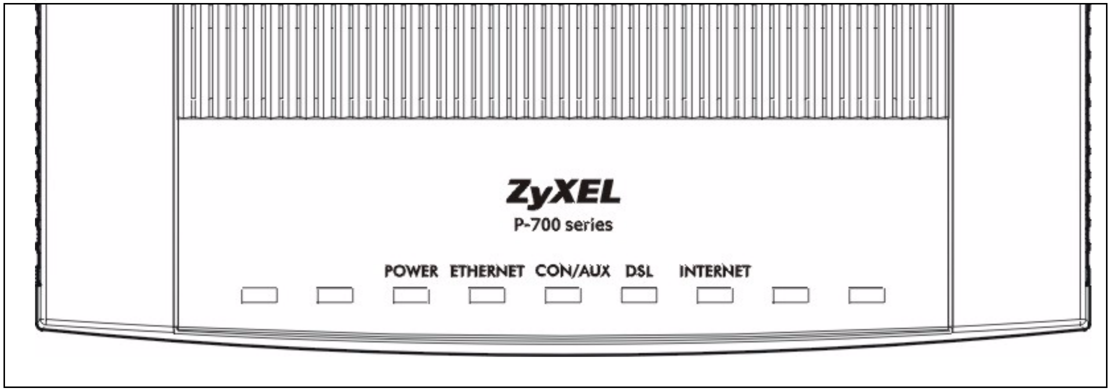
- Change the password. Use a password that’s not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.

- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.

1.4 LEDs

The following figure shows the LEDs.

Figure 3 LEDs



The following table describes the LEDs.

Table 1 LEDs

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The ZyXEL Device is receiving power and functioning properly.
		Blinking	The ZyXEL Device is rebooting or performing diagnostics.
	Red	On	Power to the ZyXEL Device is too low.
		Off	The system is not ready or has malfunctioned.
CON/AUX	Green	On	This port has a successful console connection.
	Orange	On	This port has a successful dial-up connection.
		Off	This port is not connected.
ETHERNET	Green	On	This port has a successful Ethernet connection.
		Blinking	This port is sending/receiving data.
		Off	This port is not connected.
DSL	Green	On	The DSL line is up.
		Blinking	The ZyXEL Device is initializing the DSL line.
		Off	The DSL line is down.

Table 1 LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
INTERNET	Green	On	The Internet connection is up, and the ZyXEL Device has an IP address. (If the ZyXEL Device uses RFC 1483 in bridge mode, this light does not turn on, but it does blink when the ZyXEL Device is sending/receiving data.)
		Blinking	The ZyXEL Device is sending/receiving data.
	Red	On	The ZyXEL Device tried to get an IP address, but an error occurred.
		Off	The Internet connection is down.

2

Introducing the Web Configurator

This chapter describes how to access and navigate the web configurator.

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy ZyXEL Device setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

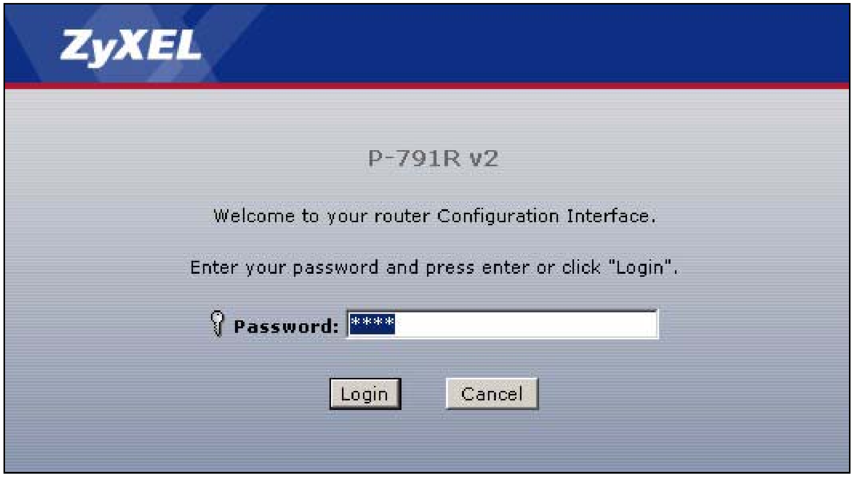
- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See the chapter on troubleshooting if you need to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

1. Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).
2. Prepare your computer/computer network to connect to the ZyXEL Device (refer to the Quick Start Guide).
3. Launch your web browser.
4. Type "192.168.1.1" as the URL.
5. A window displays as shown. Enter the default admin password **1234** to configure the wizards and the advanced features or enter the default user password **user** to view the status only. Click **Login** to proceed to a screen asking you to change your password or click **Cancel** to revert to the default password.

Figure 4 Login Screen



P-791R v2

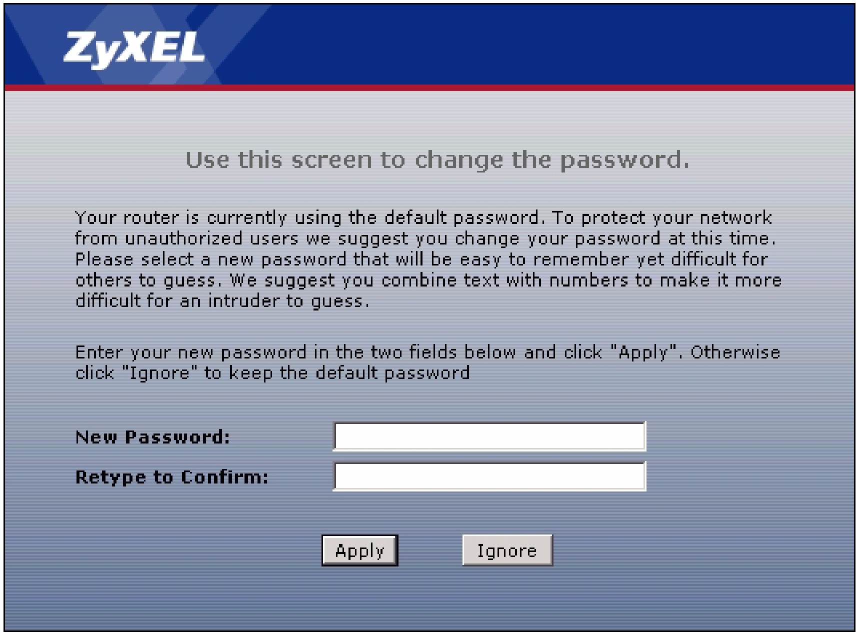
Welcome to your router Configuration Interface.

Enter your password and press enter or click "Login".

Password: ****

6 If you entered the user password, the **Status** screen appears. See Section 2.4 on page 42. If you entered the admin password, the following screen appears.

Figure 5 Change Password at Login



Use this screen to change the password.

Your router is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess. We suggest you combine text with numbers to make it more difficult for an intruder to guess.

Enter your new password in the two fields below and click "Apply". Otherwise click "Ignore" to keep the default password

New Password:

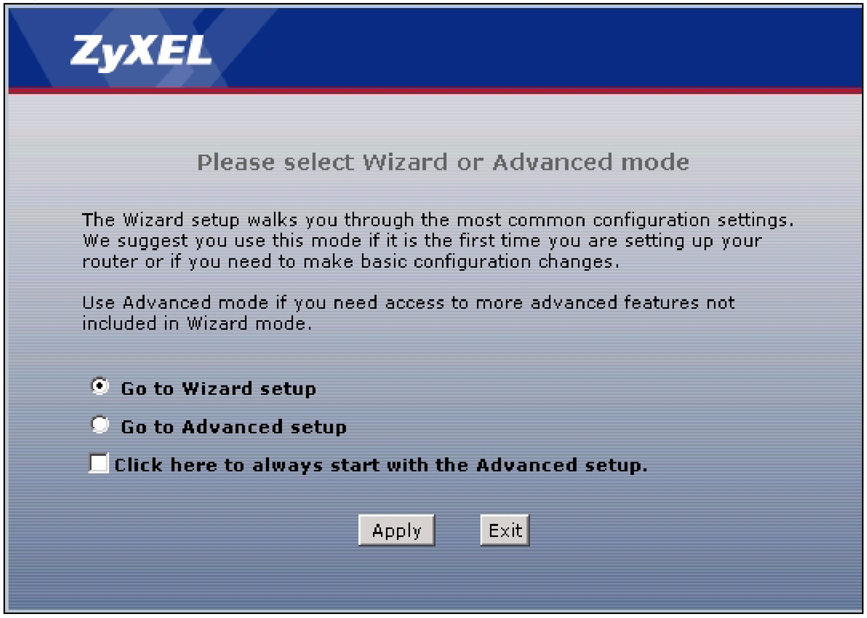
Retype to Confirm:

It is highly recommended you change the default admin password. Enter a new password between 1 and 30 characters, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.

If you do not change the password at least once, this screen appears every time you log in with the admin password. You can also change the password in System > General or in Menu 23: System Password.

7 Select **Go to Wizard setup**, and click **Apply** to display the wizard main screen. Select **Go to Advanced setup**, and click **Apply** to display the **Status** screen. Select **Click here to always start with the Advanced setup** if you want the ZyXEL Device to skip this screen from now on and always go to the **Status** screen. See Section 2.4 on page 42.

Figure 6 Select a Mode



Please select Wizard or Advanced mode

The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.

Use Advanced mode if you need access to more advanced features not included in Wizard mode.

● Go to Wizard setup

○ Go to Advanced setup

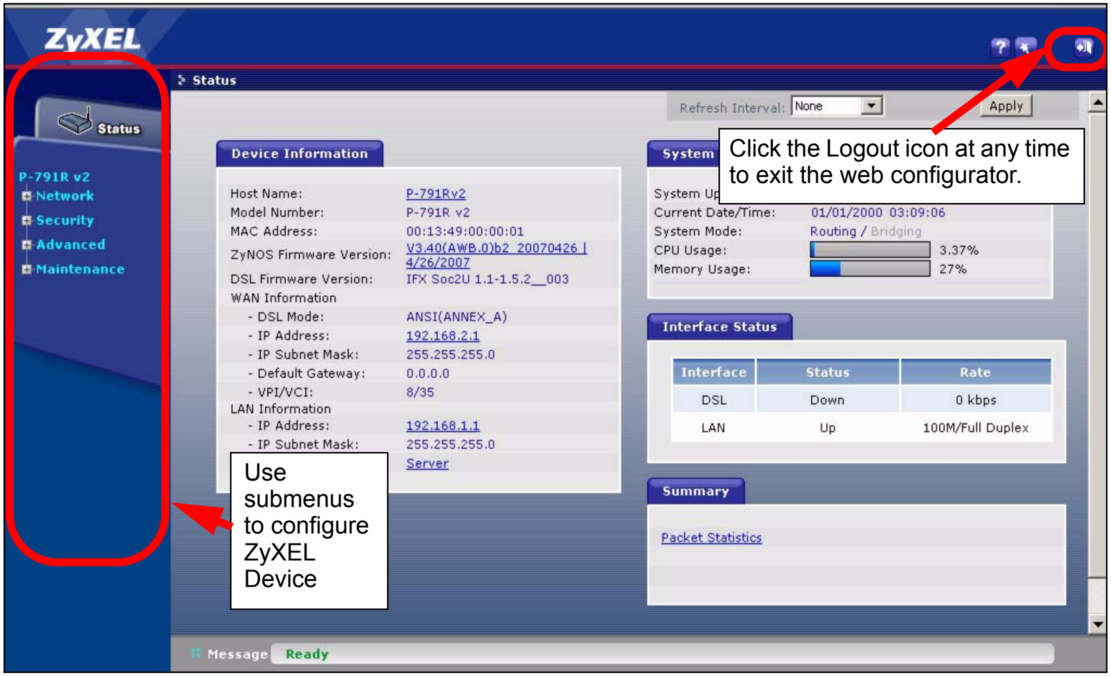
□ Click here to always start with the Advanced setup.

The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the ZyXEL Device if this happens to you.

2.3 Navigating the Web Configurator

After you enter the admin password, use the sub-menus on the navigation panel to configure ZyXEL Device features. The following table describes the sub-menus.

Figure 7 Web Configurator: Main Screen



Refresh Interval: None

Device Information

Host Name: P-791Rv2
Model Number: P-791R v2
MAC Address: 00:13:49:00:00:01
ZyNOS Firmware Version: V3.40(AWB.0)b2_20070426 | 4/26/2007
DSL Firmware Version: IFX Soc2U 1.1-1.5.2__003
WAN Information
- DSL Mode: ANSI(ANNEX_A)
- IP Address: 192.168.2.1
- IP Subnet Mask: 255.255.255.0
- Default Gateway: 0.0.0.0
- VPI/VCI: 8/35
LAN Information
- IP Address: 192.168.1.1
- IP Subnet Mask: 255.255.255.0
Server

System

System Up
Current Date/Time: 01/01/2000 03:09:06
System Mode: Routing / Bridging
CPU Usage: 3.37%
Memory Usage: 27%

Interface Status

Interface	Status	Rate
DSL	Down	0 kbps
LAN	Up	100M/Full Duplex

Summary

Packet Statistics

Click the Logout icon at any time to exit the web configurator.

Use submenus to configure ZyXEL Device

Click the ? icon (located in the top right corner of most screens) to view embedded help.

Table 2 Web Configurator Screens Summary

LINK/ICON	SUB-LINK	FUNCTION
Wizard	INTERNET SETUP	Use these screens for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
Logout		Click this icon to exit the web configurator.
Status		Use this screen to look at the ZyXEL Device's general device, system and interface status information. You can also access the summary statistics tables.
Network		
WAN	Internet Connection	Use this screen to configure ISP parameters, WAN IP address assignment, DSL line or point-to-point connections.
	More Connections	Use this screen to configure and place calls to a remote gateway.
	WAN Backup Setup	Use this screen to configure your traffic redirect properties and WAN backup settings.

Table 2 Web Configurator Screens Summary (continued)

LINK/ICON	SUB-LINK	FUNCTION
LAN	IP	Use this screen to configure LAN TCP/IP settings and other advanced properties.
	DHCP Setup	Use this screen to configure LAN DHCP settings.
	Client List	Use this screen to view current DHCP client information and to always assign an IP address to a MAC address (and host name).
	IP Alias	Use this screen to partition your LAN interface into subnets.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to configure servers behind the ZyXEL Device.
Security		
Filter	General	Use this screen to configure Internet security and apply the predefined filtering rules.
Advanced		
Static Route	Static Route	Use this screen to configure IP static routes.
Dynamic DNS	Dynamic DNS	Use this screen to set up dynamic DNS.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTPS or HTTP to manage the ZyXEL Device.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyXEL Device.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyXEL Device.
	SNMP	Use this screen to configure your ZyXEL Device’s settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyXEL Device.
	ICMP	Use this screen to change your anti-probing settings.
UPnP	General	Use this screen to enable UPnP on the ZyXEL Device.
Maintenance		
System	General	This screen contains administrative and system-related information and also allows you to change your password.
	Time Setting	Use this screen to change your ZyXEL Device’s time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your ZyXEL Device’s log settings.
Tools	Firmware	Use this screen to upload firmware to your ZyXEL Device.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your ZyXEL Device.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.

Table 2 Web Configurator Screens Summary (continued)

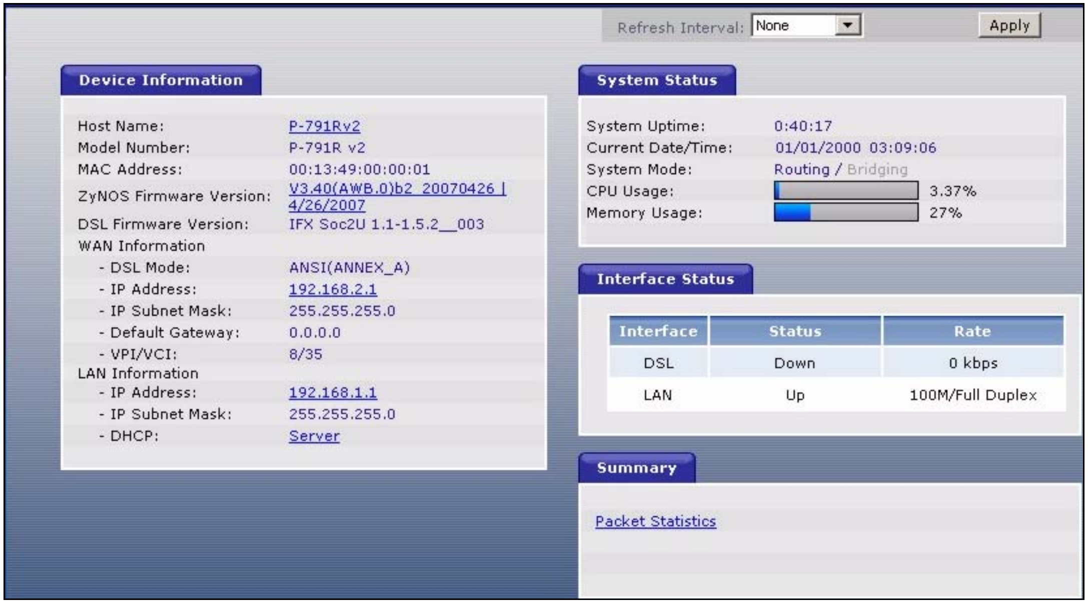
LINK/ICON	SUB-LINK	FUNCTION
Diagnostic	General	These screens display information to help you identify problems with the ZyXEL Device general connection.
	DSL Line	These screens display information to help you identify problems with the DSL line.

2.4 Status Screen

The following summarizes how to navigate the web configurator from the **Status** screen.

Some fields or links are not available if you entered the user password in the login password screen (see Figure 4 on page 38).

Figure 8 Status



Host Name: P-791Rv2
Model Number: P-791R v2
MAC Address: 00:13:49:00:00:01
ZyNOS Firmware Version: V3.40(AWB.0)b2_20070426 | 4/26/2007
DSL Firmware Version: IFX Soc2U 1.1-1.5.2__003
WAN Information
- DSL Mode: ANSI(ANNEX_A)
- IP Address: 192.168.2.1
- IP Subnet Mask: 255.255.255.0
- Default Gateway: 0.0.0.0
- VPI/VCI: 8/35
LAN Information
- IP Address: 192.168.1.1
- IP Subnet Mask: 255.255.255.0
- DHCP: Server

System Uptime: 0:40:17
Current Date/Time: 01/01/2000 03:09:06
System Mode: Routing / Bridging
CPU Usage: 3.37%
Memory Usage: 27%

Interface	Status	Rate
DSL	Down	0 kbps
LAN	Up	100M/Full Duplex

The following table describes the labels shown in the **Status** screen.

Table 3 Status

LABEL	DESCRIPTION
Refresh Interval	Select a number of seconds or **None** from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
Apply	Click this button to refresh the status screen statistics.
Device Information	
Host Name	This is the **System Name** you enter in the **Maintenance** > **System** > **General** screen. It is for identification purposes.
Model Number	This is the model name of the ZyXEL Device.

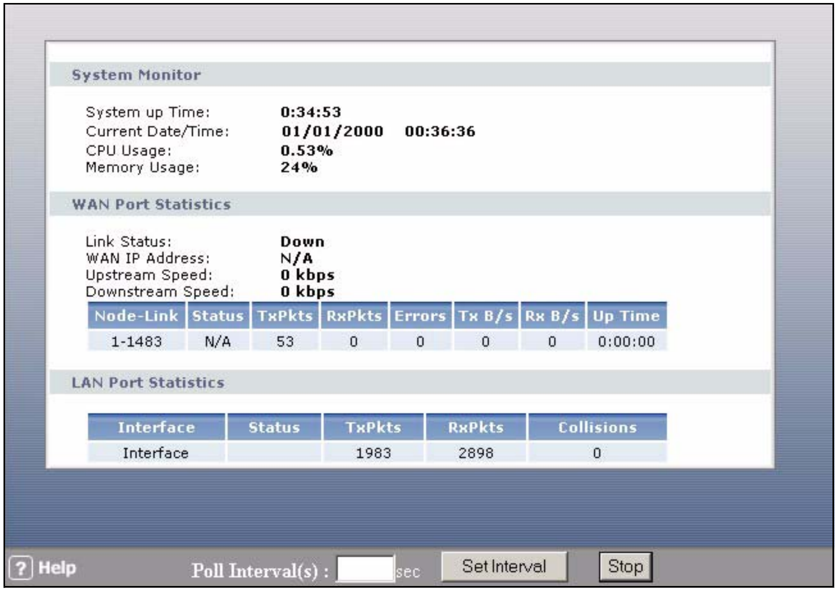
Table 3 Status (continued)

LABEL	DESCRIPTION
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
ZyNOS Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
DSL Firmware Version	This is the DSL firmware version code associated with the ZyXEL Device. This is sometimes needed by technicians to help troubleshoot problems.
WAN Information	
DSL Mode	This is the standard that your ZyXEL Device is using.
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port IP subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the Wizard or WAN screen.
LAN Information	
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the WAN port DHCP role - **Server**, **Relay** or **None**.
System Status	
System Uptime	This is the total time the ZyXEL Device has been on.
Current Date/Time	This field displays your ZyXEL Device’s present date and time.
System Mode	This displays whether the ZyXEL Device is functioning as a router or a bridge.
CPU Usage	This number shows how many kilobytes of the heap memory the ZyXEL Device is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT. The bar displays what percent of the ZyXEL Device's heap memory is in use. The bar turns from green to red when the maximum is being approached.
Memory Usage	This number shows the ZyXEL Device's total heap memory (in kilobytes). The bar displays what percent of the ZyXEL Device's heap memory is in use. The bar turns from green to red when the maximum is being approached.
Interface Status	
Interface	This displays the ZyXEL Device interfaces.
Status	This field displays **Down** (line is down), **Up** (line is up or connected) if you're using Ethernet encapsulation and **Down** (line is down), **Up** (line is up or connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation.
Rate	For the LAN port, this displays the port speed and duplex setting. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect. Simultaneous transmissions over the same port (Full-duplex) essentially double the bandwidth. For the DSL port, it displays the downstream and upstream transmission rate.
Summary	This section is not available if you use the user password to log in.
Packet Statistics	Use this screen to view port status and packet specific statistics.

2.4.1 Status: Packet Statistics

Click the **Packet Statistics** hyperlink in the **Status** screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

Figure 9 Status > Packet Statistics



System Monitor

System up Time: 0:34:53
Current Date/Time: 01/01/2000 00:36:36
CPU Usage: 0.53%
Memory Usage: 24%

WAN Port Statistics

Link Status: Down
WAN IP Address: N/A
Upstream Speed: 0 kbps
Downstream Speed: 0 kbps

Node-Link	Status	TxPkts	RxPkts	Errors	Tx B/s	Rx B/s	Up Time
1-1483	N/A	53	0	0	0	0	0:00:00

LAN Port Statistics

Interface	Status	TxPkts	RxPkts	Collisions
Interface		1983	2898	0

The following table describes the fields in this screen.

Table 4 Status > Packet Statistics

LABEL	DESCRIPTION
System Monitor	
System up Time	This is the elapsed time the system has been up.
Current Date/Time	This field displays your ZyXEL Device's present date and time.
CPU Usage	This field specifies the percentage of CPU utilization.
Memory Usage	This field specifies the percentage of memory utilization.
WAN Port Statistics	
Link Status	This is the status of your WAN link.
WAN IP Address	This is the IP address assigned to your ZyXEL Device on the WAN.
Upstream Speed	This is the upstream speed of your ZyXEL Device.
Downstream Speed	This is the downstream speed of your ZyXEL Device.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
Status	This field displays **Down** (line is down), **Up** (line is up or connected) if you're using Ethernet encapsulation and **Down** (line is down), **Up** (line is up or connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation. It displays **N/A** if the port is not connected.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.

Table 4 Status > Packet Statistics (continued)

LABEL	DESCRIPTION
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
LAN Port Statistics	
Interface	This field displays the type of port.
Status	This field displays **Down** (line is down), **Up** (line is up or connected) if you're using Ethernet encapsulation and **Down** (line is down), **Up** (line is up or connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Collisions	This is the number of collisions on this port.
Help	Click this to open the embedded help.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval** field above.
Stop	Click this button to halt the refreshing of the system statistics.

2.5 Resetting the ZyXEL Device

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the ZyXEL Device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to “1234”.

2.5.1 Using the Reset Button

1 Make sure the **POWER** LED is on (not blinking).

2 Press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the ZyXEL Device restarts.

3

Wizard Setup for Internet Access

This chapter provides information on the Wizard Setup screens for Internet access in the web configurator.

3.1 Introduction

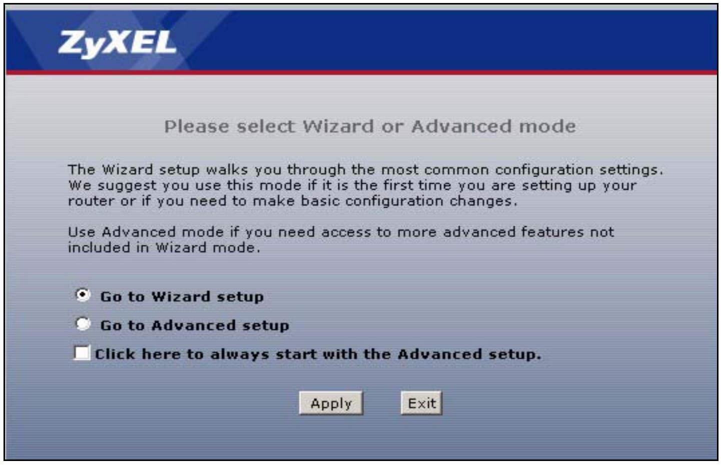
Use the wizard setup screens to configure your system for Internet access with the information given to you by your ISP.

See the advanced menu chapters for background information on these fields.

3.2 Internet Access Wizard Setup

1 After you enter the admin password to access the web configurator, select **Go to Wizard setup** and click **Apply**. Otherwise, click the wizard icon (🪄) in the top right corner of the web configurator to display the wizard main screen.

Figure 10 Select a Mode



Please select Wizard or Advanced mode

The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router or if you need to make basic configuration changes.

Use Advanced mode if you need access to more advanced features not included in Wizard mode.

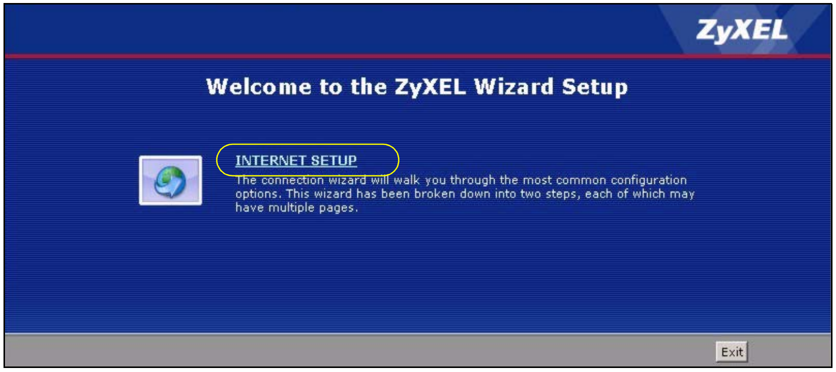
● Go to Wizard setup

○ Go to Advanced setup

□ Click here to always start with the Advanced setup.

2 Click **INTERNET SETUP** to configure the system for Internet access.

Figure 11 Wizard: Welcome



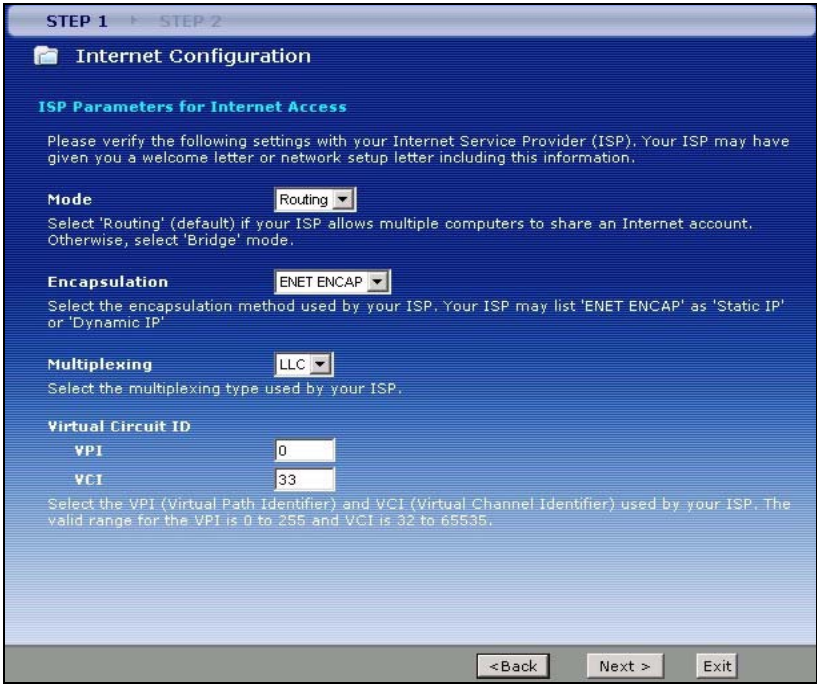
Welcome to the ZyXEL Wizard Setup

INTERNET SETUP

The connection wizard will walk you through the most common configuration options. This wizard has been broken down into two steps, each of which may have multiple pages.

3 Type the Internet access information given to you by your ISP exactly in the wizard screen. If not given, leave the fields set to the default.

Figure 12 Internet Access Wizard Setup: ISP Parameters



Internet Configuration

ISP Parameters for Internet Access

Please verify the following settings with your Internet Service Provider (ISP). Your ISP may have given you a welcome letter or network setup letter including this information.

Mode: Routing

Select 'Routing' (default) if your ISP allows multiple computers to share an Internet account. Otherwise, select 'Bridge' mode.

Encapsulation: ENET ENCAP

Select the encapsulation method used by your ISP. Your ISP may list 'ENET ENCAP' as 'Static IP' or 'Dynamic IP'

Multiplexing: LLC

Select the multiplexing type used by your ISP.

Virtual Circuit ID

VPI: 0

VCI: 33

Select the VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) used by your ISP. The valid range for the VPI is 0 to 255 and VCI is 32 to 65535.

The following table describes the fields in this screen.

Table 5 Internet Access Wizard Setup: ISP Parameters

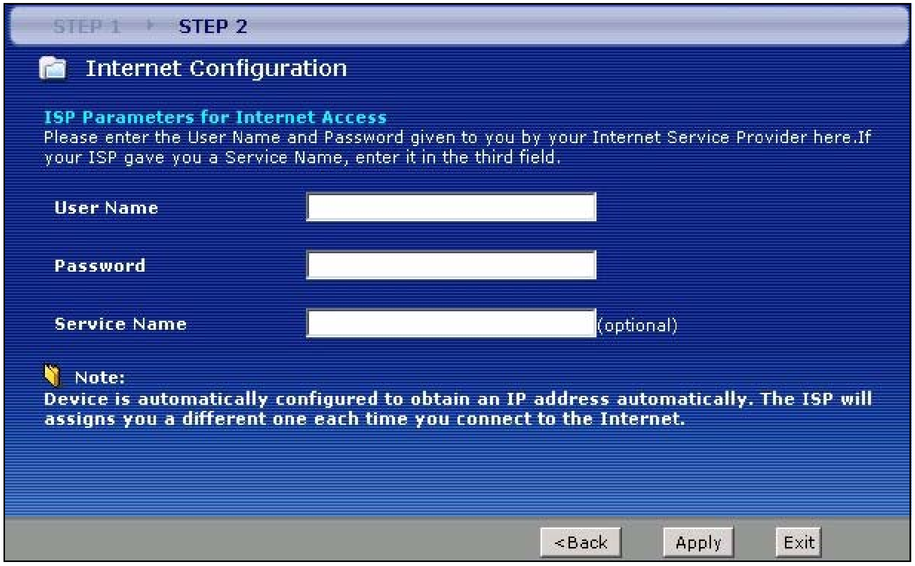
LABEL	DESCRIPTION
Mode	From the **Mode** drop-down list box, select **Routing** (default) if your ISP allows multiple computers to share an Internet account. Otherwise select **Bridge**.
Encapsulation	Select the encapsulation type your ISP uses from the **Encapsulation** drop-down list box. Choices vary depending on what you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.
Multiplexing	Select the multiplexing method used by your ISP from the **Multiplex** drop-down list box either VC-based or LLC-based.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.

Table 5 Internet Access Wizard Setup: ISP Parameters

LABEL	DESCRIPTION
VPI	Enter the VPI assigned to you. This field may already be configured.
VCI	Enter the VCI assigned to you. This field may already be configured.
Back	Click **Back** to go back to the previous screen.
Next	Click **Next** to continue to the next wizard screen. The next wizard screen you see depends on what protocol you chose above.
Exit	Click **Exit** to close the wizard screen without saving your changes.

4 The next wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue.

Figure 13 Internet Connection with PPPoE



ISP Parameters for Internet Access

Please enter the User Name and Password given to you by your Internet Service Provider here.If your ISP gave you a Service Name, enter it in the third field.

User Name

Password

Service Name (optional)

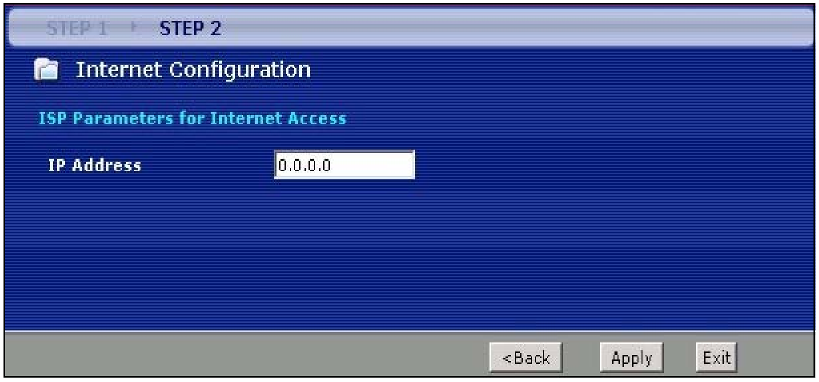
Note:
Device is automatically configured to obtain an IP address automatically. The ISP will assigns you a different one each time you connect to the Internet.

The following table describes the fields in this screen.

Table 6 Internet Connection with PPPoE

LABEL	DESCRIPTION
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
Service Name	Type the name of your PPPoE service here.
Back	Click **Back** to go back to the previous wizard screen.
Apply	Click **Apply** to save your changes to the ZyXEL Device.
Exit	Click **Exit** to close the wizard screen without saving your changes.

Figure 14 Internet Connection with RFC 1483



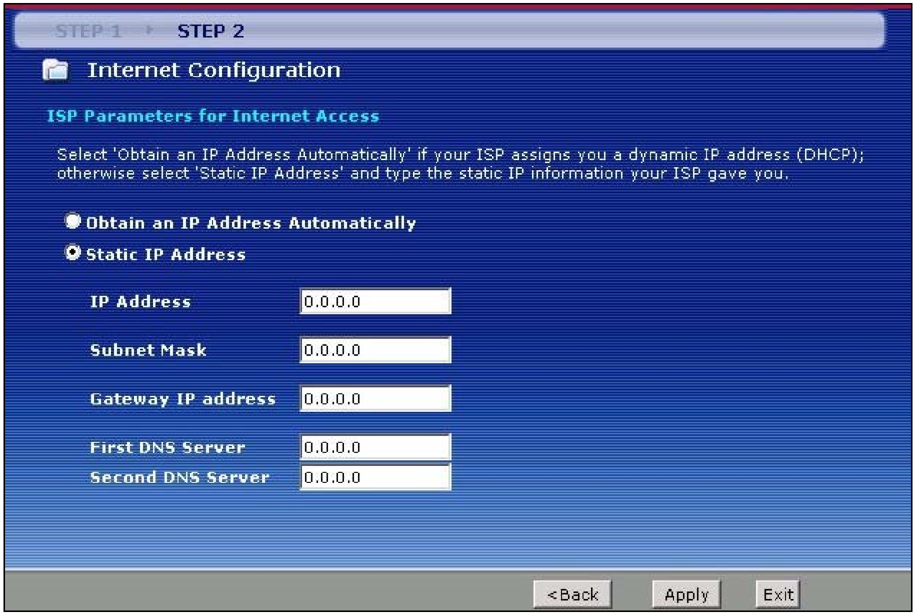
IP Address 0.0.0.0

The following table describes the fields in this screen.

Table 7 Internet Connection with RFC 1483

LABEL	DESCRIPTION
IP Address	This field is available if you select **Routing** in the **Mode** field. Type your ISP assigned IP address in this field.
Back	Click **Back** to go back to the previous wizard screen.
Next	Click **Next** to continue to the next wizard screen.
Exit	Click **Exit** to close the wizard screen without saving your changes.

Figure 15 Internet Connection with ENET ENCAP



Select 'Obtain an IP Address Automatically' if your ISP assigns you a dynamic IP address (DHCP); otherwise select 'Static IP Address' and type the static IP information your ISP gave you.

○ Obtain an IP Address Automatically
● Static IP Address

IP Address 0.0.0.0
Subnet Mask 0.0.0.0
Gateway IP address 0.0.0.0
First DNS Server 0.0.0.0
Second DNS Server 0.0.0.0

The following table describes the fields in this screen.

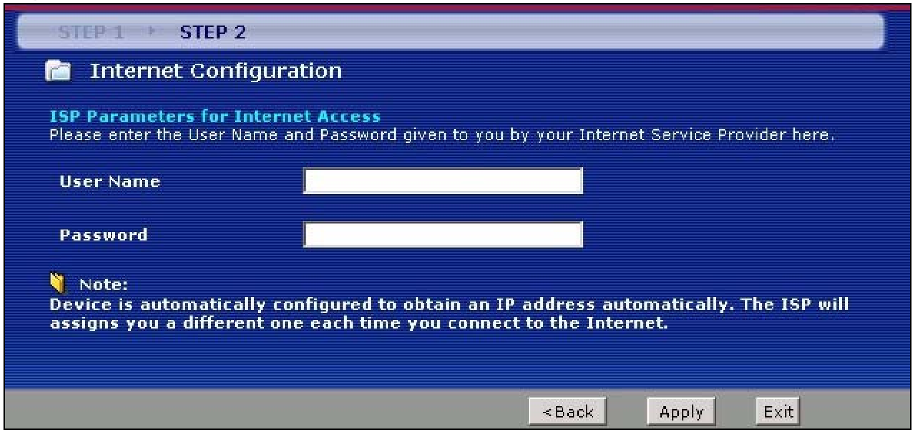
Table 8 Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select **Obtain an IP Address Automatically** if you have a dynamic IP address.
Static IP Address	Select **Static IP Address** if your ISP gives you a fixed IP address.

Table 8 Internet Connection with ENET ENCAP (continued)

LABEL	DESCRIPTION
IP Address	Enter your ISP assigned IP address.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the appendices to calculate a subnet mask If you are implementing subnetting.
Gateway IP address	You must specify a gateway IP address (supplied by your ISP) when you use **ENET ENCAP** in the **Encapsulation** field in the previous screen.
First DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Second DNS Server	As above.
Back	Click **Back** to go back to the previous wizard screen.
Apply	Click **Apply** to save your changes to the ZyXEL Device.
Exit	Click **Exit** to close the wizard screen without saving your changes.

Figure 16 Internet Connection with PPPoA



ISP Parameters for Internet Access

Please enter the User Name and Password given to you by your Internet Service Provider here.

User Name

Password

Note:
Device is automatically configured to obtain an IP address automatically. The ISP will assigns you a different one each time you connect to the Internet.

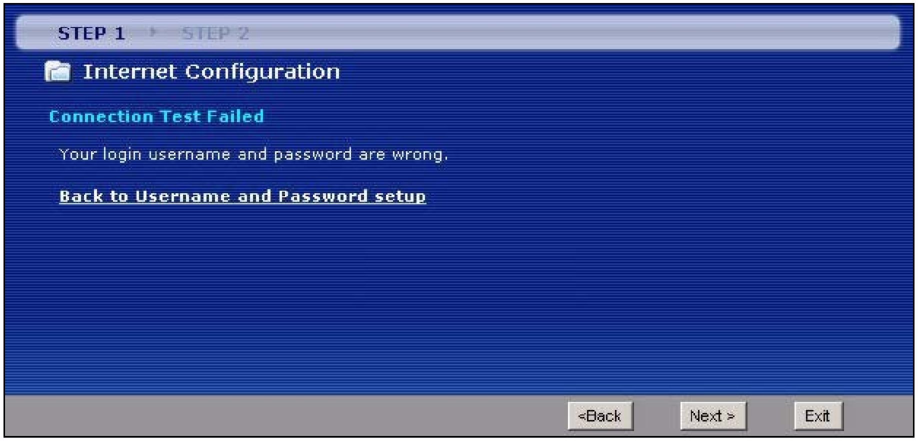
The following table describes the fields in this screen.

Table 9 Internet Connection with PPPoA

LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
Back	Click **Back** to go back to the previous wizard screen.
Apply	Click **Apply** to save your changes to the ZyXEL Device.
Exit	Click **Exit** to close the wizard screen without saving your changes.

- If the user name and/or password you entered for PPPoE or PPPoA connection are not correct, the screen displays as shown next. Click **Back to Username and Password setup** to go back to the screen where you can modify them.

Figure 17 Connection Test Failed-1



Internet Configuration

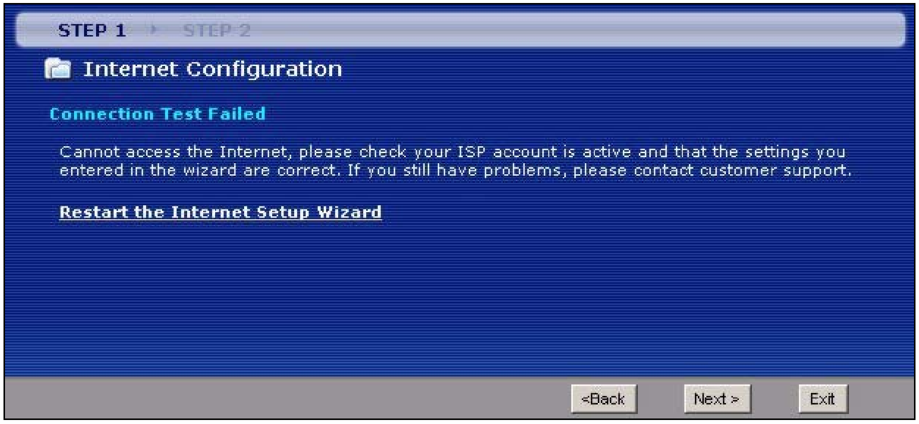
Connection Test Failed

Your login username and password are wrong.

Back to Username and Password setup

- If the following screen displays, check if your account is activated or click **Restart the Internet Setup Wizard** to verify your Internet access settings.

Figure 18 Connection Test Failed-2.



Internet Configuration

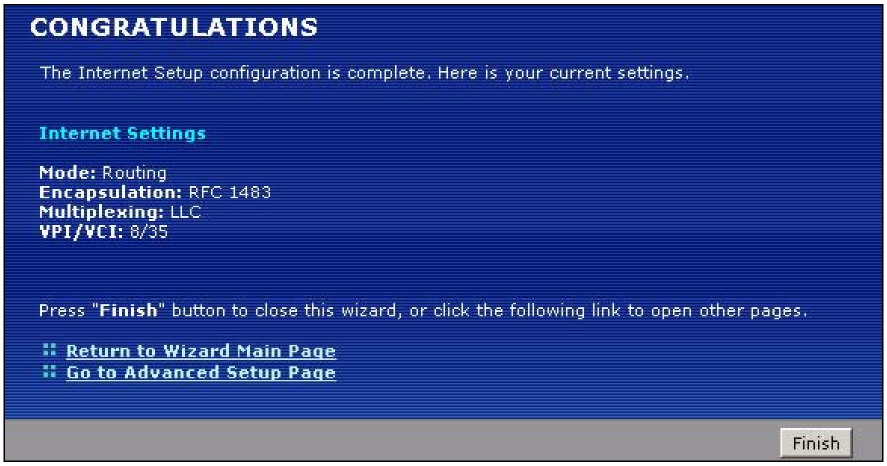
Connection Test Failed

Cannot access the Internet, please check your ISP account is active and that the settings you entered in the wizard are correct. If you still have problems, please contact customer support.

Restart the Internet Setup Wizard

When you are finished with the Internet Setup Wizard the following screen displays your configuration details. Click **Finish** to exit the wizard.

Figure 19 Internet Setup Wizard Finished



CONGRATULATIONS

The Internet Setup configuration is complete. Here is your current settings.

Internet Settings

Mode: Routing
Encapsulation: RFC 1483
Multiplexing: LLC
VPI/VCI: 8/35

Press "**Finish**" button to close this wizard, or click the following link to open other pages.

- Return to Wizard Main Page
- Go to Advanced Setup Page

4

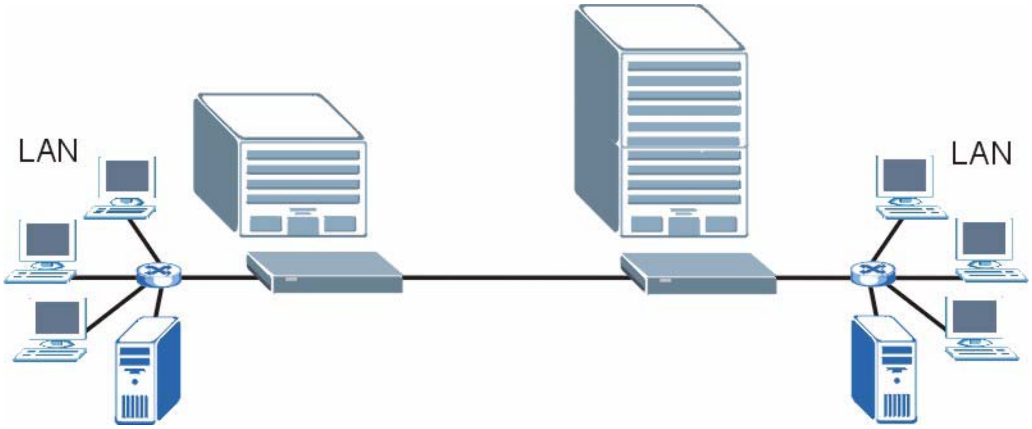
Point-to-point Configuration

This chapter introduces point-to-point connections.

4.1 Overview

You can set up point-to-point connection between two ZyXEL Devices. These connections offer a cost-effective, high-speed connection for high-bandwidth applications such as videoconferencing and distance learning. An example is shown below.

Figure 20 Example: Point-to-point Connections



In a point-to-point connection, the DSL ports on the ZyXEL Devices are directly connected to each other, not to an ISP or the Internet.

A point-to-point connection can use RFC 1483 in bridge mode or ENET ENCAP in router mode.

In a point-to-point connection, the ZyXEL Devices should use the same VPI, VCI, multiplexing, and encapsulation method.

To establish a point-to-point connection, one of the ZyXEL Devices becomes the server (instead of the ISP). The server controls some of the attributes of the DSL connection, such as the transfer rate and the DSL operational mode. Otherwise, there is no difference between the server and the client. Either one can initiate the point-to-point connection.

You can only establish point-to-point connections between ZyXEL Devices that support this kind of server/client mode.

4.2 Point-to-point Connection Procedure

Follow these directions to set up a point-to-point connection.

1 Set up the Server.

2 Set up the Client.

3 Connect the ZyXEL Devices.

4.2.1 Set up the Server

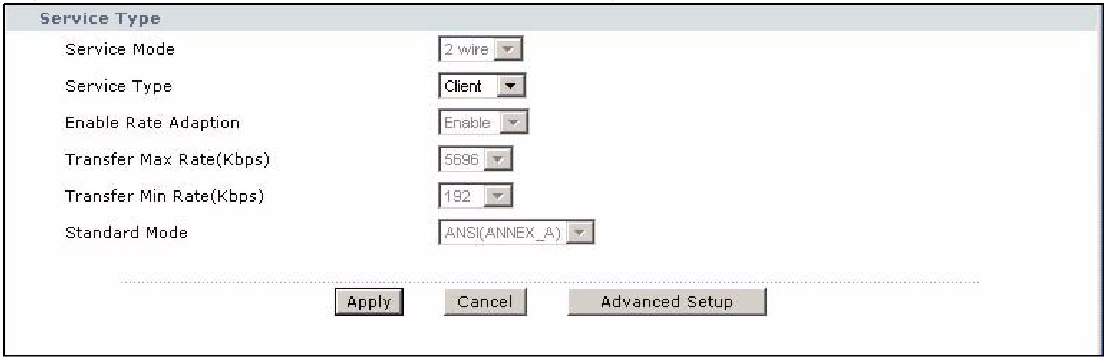
1 Log in to the ZyXEL Device that will be the server. (See Chapter 2 on page 37.)

2 Click **Network** > **WAN** > **Internet Connection**.

3 Configure the **VPI**, **VCI**, **Multiplexing**, and **Encapsulation** fields for the point-to-point connection. In the **Encapsulation** field, select either **RFC 1483** or **ENET ENCAP**.

4 Scroll down to the **Service Type** section. The following screen appears.

Figure 21 WAN > Internet Connection > Service Type



Service Type

Service Mode	2 wire
Service Type	Client
Enable Rate Adaption	Enable
Transfer Max Rate(Kbps)	5696
Transfer Min Rate(Kbps)	192
Standard Mode	ANSI(ANNEX_A)

5 In the **Service Type** field, select **Server**. The rest of the fields are enabled.

6 Configure the rest of the fields, if necessary. For example, you might want to set the **Transfer Max Rate** to the maximum value.

7 Click **Apply**.

4.2.2 Set up the Client

1 Log in to the ZyXEL Device that will be the client. (See Chapter 2 on page 37.)

2 Click **Network** > **WAN** > **Internet Connection**.

3 Set the **VPI**, **VCI**, **Multiplexing**, and **Encapsulation** to the same values you set in the server.

4 Scroll down to the **Service Type** section. See Figure 21 on page 56 above.

5 In the **Service Mode** field, select the same type of connection you selected for the server.

6 In the **Service Type** field, select **Client**. The rest of the fields will be negotiated with the server.

7 Click **Apply**.

4.2.3 Connect the ZyXEL Devices

Connect the **DSL** ports on the ZyXEL Devices together, and wait while the ZyXEL Devices automatically establish the connection. When the connection is established, the **DSL** and **INTERNET** lights are on. It takes up to half a minute to establish the connection. If the ZyXEL Devices do not establish the connection, verify that the settings (except the **Service Type**) match.

PART II
Network Setup

5

WAN Setup

This chapter describes how to configure WAN settings.

5.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

5.1.1 Encapsulation

Be sure to use the encapsulation method required by your ISP. The ZyXEL Device supports the following methods.

5.1.1.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the **ENET ENCAP Gateway** field in the second wizard screen. You can get this information from your ISP.

5.1.1.2 PPP over Ethernet

PPPoE (Point-to-Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyXEL Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyXEL Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

5.1.1.3 PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The ZyXEL Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (DSL Access Multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

5.1.1.4 RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to the RFC for more detailed information.

5.1.2 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

5.1.2.1 VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

5.1.2.2 LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

5.1.3 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

5.1.4 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and ENET ENCAP gateway.

5.1.4.1 IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the **IP Address** and **ENET ENCAP Gateway** fields are not applicable (N/A). If you have a static IP, then you *only* need to fill in the **IP Address** field and *not* the **ENET ENCAP Gateway** field.

5.1.4.2 IP Assignment with RFC 1483 Encapsulation

In this case the IP Address Assignment *must* be static with the same requirements for the **IP Address** and **ENET ENCAP Gateway** fields as stated above.

5.1.4.3 IP Assignment with ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the **IP Address** and **ENET ENCAP Gateway** fields as supplied by your ISP. However for a dynamic IP, the ZyXEL Device acts as a DHCP client on the WAN port and so the **IP Address** and **ENET ENCAP Gateway** fields are not applicable (N/A) as the DHCP server assigns them to the ZyXEL Device.

5.1.5 Nailed-Up Connection (PPP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyXEL Device does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyXEL Device will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern

5.1.6 NAT

NAT (Network Address Translation, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

5.2 Metric

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

The metric sets the priority for the ZyXEL Device's routes to the Internet. If any two of the default routes have the same metric, the ZyXEL Device uses the following pre-defined priorities:

- Normal route: designated by the ISP (see Section 5.4 on page 65)
- Traffic-redirect route (see Section 5.6 on page 74)
- WAN-backup route, also called dial-backup (see Section 5.9 on page 75)

For example, if the normal route has a metric of "1" and the traffic-redirect route has a metric of "2" and dial-backup route has a metric of "3", then the normal route acts as the primary default route. If the normal route fails to connect to the Internet, the ZyXEL Device tries the traffic-redirect route next. In the same manner, the ZyXEL Device uses the dial-backup route if the traffic-redirect route also fails.

If you want the dial-backup route to take first priority over the traffic-redirect route or even the normal route, all you need to do is set the dial-backup route's metric to "1" and the others to "2" (or greater).

IP Policy Routing overrides the default routing behavior and takes priority over all of the routes mentioned above.

5.3 Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

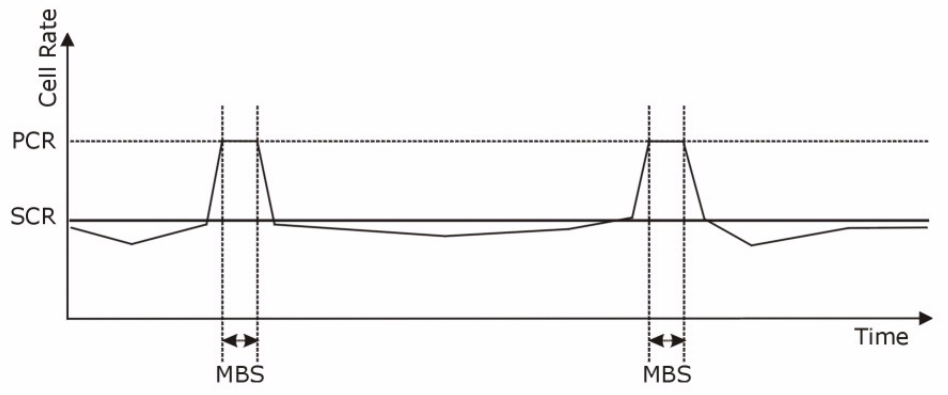
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 22 Example of Traffic Shaping



5.3.1 ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

5.3.1.1 Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

5.3.1.2 Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

5.3.1.3 Unspecified Bit Rate (UBR)

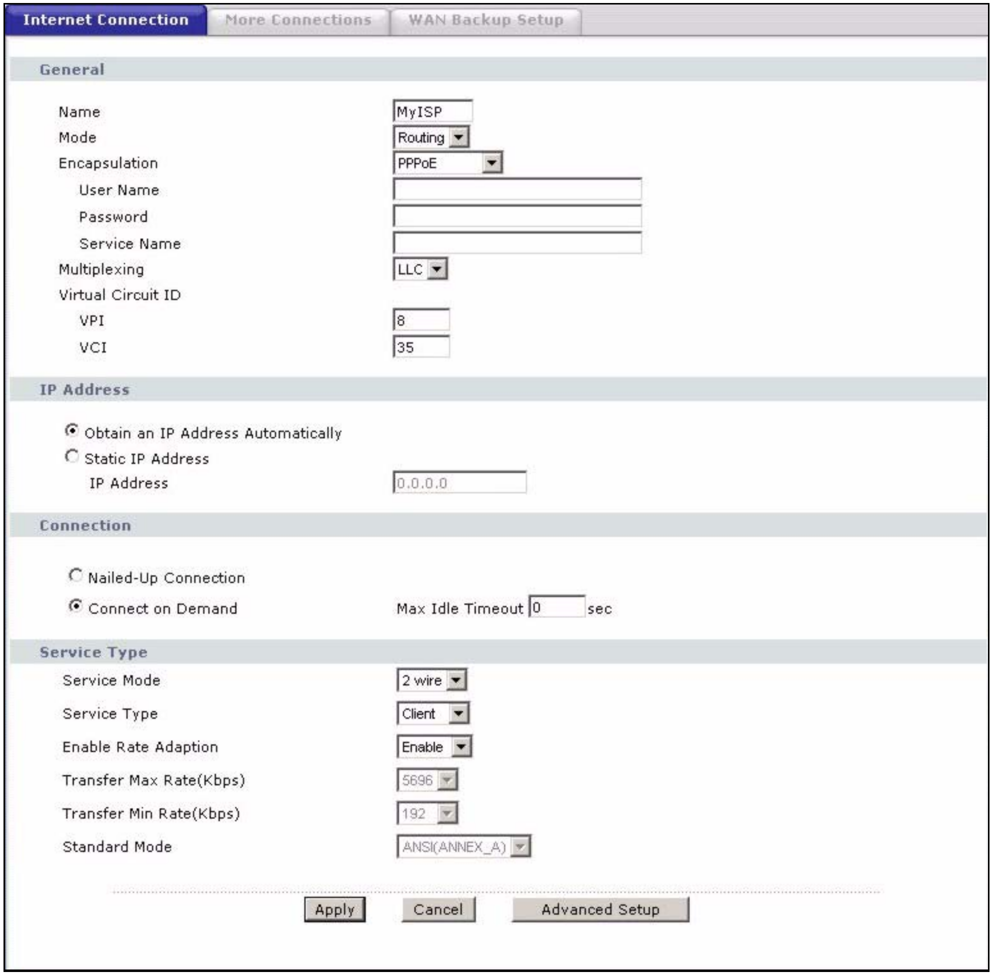
The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

5.4 Internet Connection

To change your ZyXEL Device’s WAN remote node settings, click **Network > WAN > Internet Connection**. The screen differs by the encapsulation.

See Section 5.1 on page 61 for more information.

Figure 23 WAN > Internet Connection



General

Name: MyISP
Mode: Routing
Encapsulation: PPPoE
User Name:
Password:
Service Name:
Multiplexing: LLC
Virtual Circuit ID
VPI: 8
VCI: 35

IP Address

● Obtain an IP Address Automatically
○ Static IP Address
IP Address: 0.0.0.0

Connection

○ Nailed-Up Connection
● Connect on Demand   Max Idle Timeout 0 sec

Service Type

Service Mode: 2 wire
Service Type: Client
Enable Rate Adaption: Enable
Transfer Max Rate(Kbps): 5696
Transfer Min Rate(Kbps): 192
Standard Mode: ANSI(ANNEX_A)

The following table describes the labels in this screen.

Table 10 WAN > Internet Connection

LABEL	DESCRIPTION
General	
Name	Enter the name of your Internet Service Provider, for example "MyISP". This information is for descriptive purposes only.
Mode	Select **Routing** (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select **Bridge**.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**. If you set up a point-to-point or a point-to-2points connection, select either **ENET ENCAP** or **RFC 1483**.
User Name	(PPPoA and PPPoE only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE only) Enter the password associated with the user name above.

Table 10 WAN > Internet Connection (continued)

LABEL	DESCRIPTION
Service Name	(PPPoE only) Type the name of your PPPoE service here.
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	These fields only appear if the **Mode** is **Routing**. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. ‘
Obtain an IP Address Automatically	(PPPoE, PPPoA, and ENET ENCAP only) Select this if you have a dynamic IP address.
Static IP Address	(PPPoE, PPPoA, and ENET ENCAP only) Select this if you do not have a dynamic IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	(ENET ENCAP only) This field is enabled if you select **Static IP Address**. Enter the subnet mask provided by your ISP.
Gateway IP Address	(ENET ENCAP only) This field is enabled if you select **Static IP Address**. Enter the gateway IP address provided by your ISP. You must enter a valid IP address for Internet access. If you enter 0.0.0.0, the Internet connection does not work.
Connection	This section only appears if the **Encapsulation** is **PPPoE** and **PPPoA**.
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
Service Type	
Service Mode	This field indicates that the ZyXEL Device uses **2-wire** mode for the DSL connection. In **2-wire** mode, the maximum data rate is up to 5.69 Mbps. This field is not configurable.
Service Type	Indicate whether the ZyXEL Device is the server or the client in the DSL connection. Select **Server** if this ZyXEL Device is the server in a point-to-point application. (See Chapter 4 on page 55.) Otherwise, select **Client**.
Enable Rate Adaption	This field is enabled if **Service Type** is **Server**. Indicate whether or not the ZyXEL Device can adjust the speed of its connection to that of the other device.
Transfer Max Rate (Kbps)	This field is enabled if **Service Type** is **Server**. Set the maximum rate at which the ZyXEL Device sends and receives information. The actual transfer rate will be between this value and the minimum transfer rate you configure.
Transfer Min Rate (Kbps)	This field is enabled if **Service Type** is **Server**. Set the minimum rate at which the ZyXEL Device sends and receives information. The actual transfer rate will be between this value and the maximum transfer rate you configure.

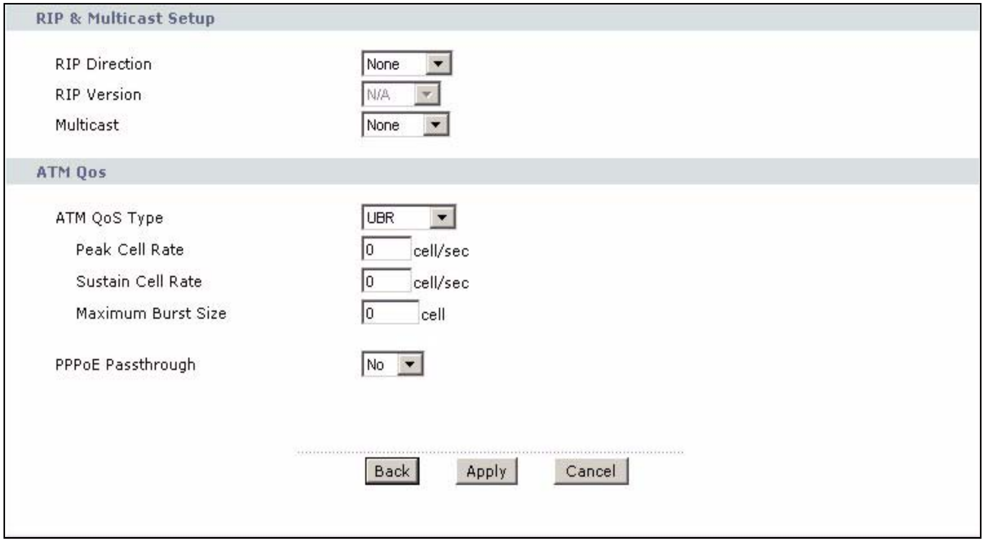
Table 10 WAN > Internet Connection (continued)

LABEL	DESCRIPTION
Standard Mode	This field is enabled if **Service Type** is **Server**. Select the operational mode the ZyXEL Device uses in the DSL connection. Annex A refers to connections over POTS and Annex B refers to connections over ISDN lines.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Advanced Setup	Click this button to display the **Advanced WAN Setup** screen and edit more details of your WAN setup.

5.4.1 Configuring Advanced Internet Connection

Use this screen to edit your ZyXEL Device's advanced settings for Internet connections. Click the **Advanced Setup** button in the **Internet Connection** screen. The screen appears as shown.

Figure 24 WAN > Internet Connection > Advanced Setup



RIP & Multicast Setup

RIP Direction: None
RIP Version: N/A
Multicast: None

ATM Qos

ATM QoS Type: UBR
Peak Cell Rate: 0 cell/sec
Sustain Cell Rate: 0 cell/sec
Maximum Burst Size: 0 cell

PPPoE Passthrough: No

The following table describes the labels in this screen.

Table 11 WAN > Internet Connection > Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyXEL Device will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

Table 11 WAN > Internet Connection > Advanced Setup (continued)

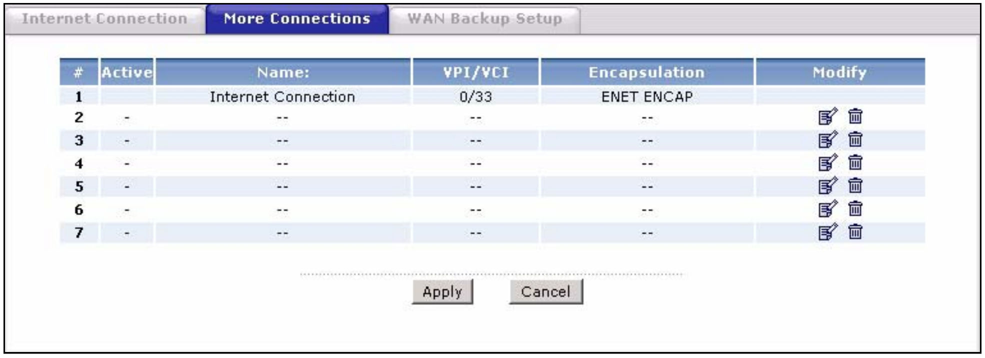
LABEL	DESCRIPTION
RIP Version	This field is enabled if **RIP Direction** is not **None**. The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Select **None** to disable it.
ATM QoS	
ATM QoS Type	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR-nRT** (Variable Bit Rate-non Real Time) or **VBR-RT** (Variable Bit Rate-Real Time) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
PPPoE Passthrough	This field is only effective for PPPoE connections. In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE Passthrough to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for applications where NAT is not appropriate. Disable PPPoE passthrough if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

5.5 Configuring More Connections

This section describes the protocol-independent parameters for a remote network. They are required for placing calls to a remote gateway and the network behind it across a WAN connection. When you use the **WAN > Internet Connection** screen to set up Internet access, you are configuring the first WAN connection.

Click **Network > WAN > More Connections** to display the screen as shown next.

Figure 25 WAN > More Connections



#	Active	Name:	VPI/VCI	Encapsulation	Modify
1		Internet Connection	0/33	ENET ENCAP	
2	-	--	--	--	✎ 🗑
3	-	--	--	--	✎ 🗑
4	-	--	--	--	✎ 🗑
5	-	--	--	--	✎ 🗑
6	-	--	--	--	✎ 🗑
7	-	--	--	--	✎ 🗑

The following table describes the labels in this screen.

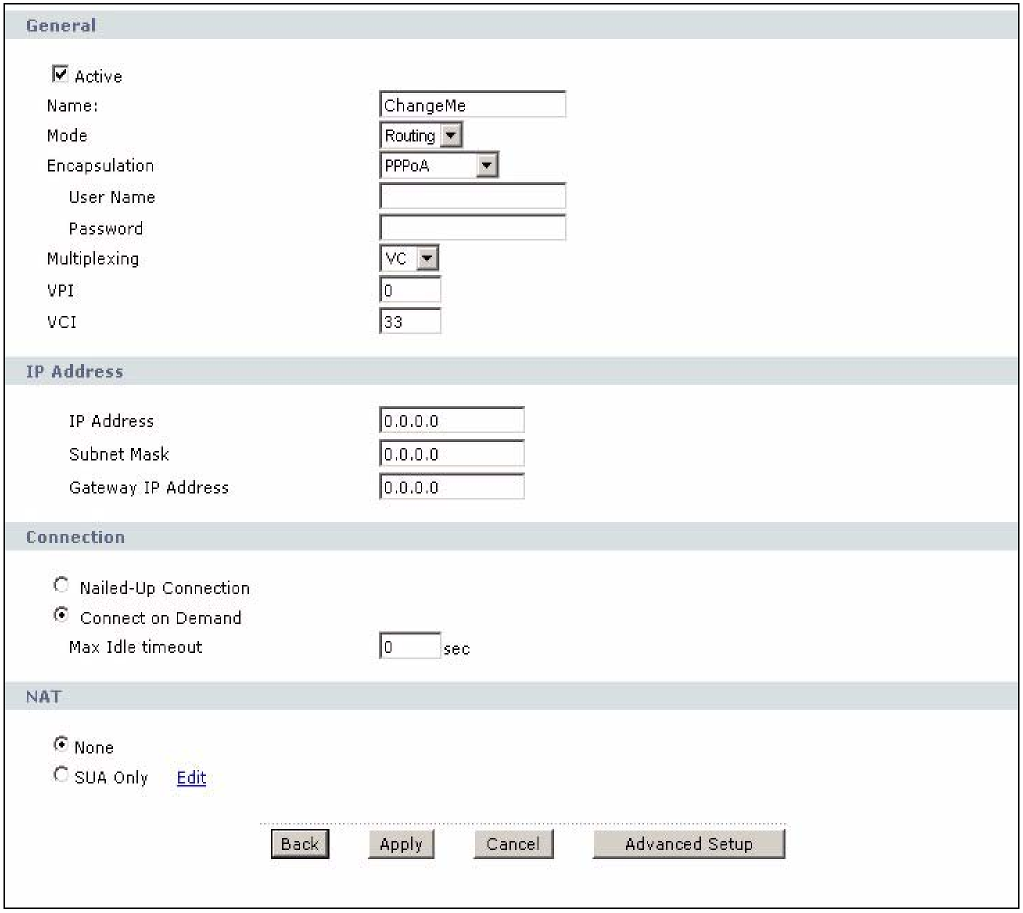
Table 12 WAN > More Connections

LABEL	DESCRIPTION
#	This is the index number of a connection.
Active	This display whether this connection is activated. Clear the check box to disable the connection. Select the check box to enable it.
Name	This is the descriptive name for this connection.
VPI/VCI	This is the VPI and VCI values used for this connection.
Encapsulation	This is the method of encapsulation used for this connection.
Modify	The first (ISP) connection is read-only in this screen. Use the **WAN > Internet Connection** screen to edit it. Click the edit icon to go to the screen where you can edit the connection. Click the delete icon to remove an existing connection. You cannot remove the first connection.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

5.5.1 More Connections Edit

Use this screen to configure a connection. Click the edit icon in the **More Connections** screen.

Figure 26 WAN > More Connections > Edit



General

☑ Active

Name: ChangeMe

Mode: Routing

Encapsulation: PPPoA

User Name:

Password:

Multiplexing: VC

VPI: 0

VCI: 33

IP Address

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway IP Address: 0.0.0.0

Connection

○ Nailed-Up Connection

● Connect on Demand

Max Idle timeout: 0 sec

NAT

● None

○ SUA Only Edit

The following table describes the labels in this screen.

Table 13 WAN > More Connections > Edit

LABEL	DESCRIPTION
General	
Active	Select the check box to activate or clear the check box to deactivate this connection.
Name	Enter a unique, descriptive name of up to 13 ASCII characters for this connection.
Mode	Select **Routing** from the drop-down list box if your ISP allows multiple computers to share an Internet account. If you select **Bridge**, the ZyXEL Device will forward any packet that it does not route to this remote node; otherwise, the packets are discarded.
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices are **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**. If you set up a point-to-point connection, select either **ENET ENCAP** or **RFC 1483**.
User Name	(PPPoA and PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoA and PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.

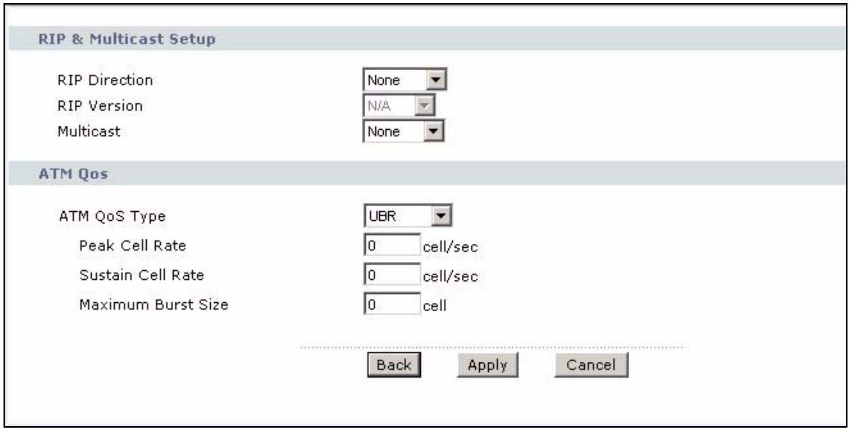
Table 13 WAN > More Connections > Edit (continued)

LABEL	DESCRIPTION
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**. By prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. If you select VC, specify separate VPI and VCI numbers for each protocol. For LLC-based multiplexing or PPP encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header. In this case, only one set of VPI and VCI numbers need be specified for all protocols.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
IP Address	These fields only appear if the **Mode** is **Routing**. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. ‘
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Address	Enter the gateway IP address provided by your ISP.
Connection	This section only appears if the **Encapsulation** is **PPPoE** and **PPPoA**.
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
NAT	**SUA Only** is available only when you select **Routing** in the **Mode** field. Select **SUA Only** if you have one public IP address and want to use NAT. Click **Edit** to go to the **Port Forwarding** screen to edit a server mapping set. Otherwise, select **None** to disable NAT.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Advanced Setup	Click this button to display the **More Connections Advanced** screen and edit more details of your WAN setup.

5.5.2 Configuring More Connections Advanced Setup

Use this screen to edit your ZyXEL Device's advanced WAN settings. Click the **Advanced Setup** button in the **More Connections Edit** screen. The screen appears as shown.

Figure 27 WAN > More Connections > Advanced Setup



RIP & Multicast Setup

RIP Direction: None

RIP Version: N/A

Multicast: None

ATM Qos

ATM QoS Type: UBR

Peak Cell Rate: 0 cell/sec

Sustain Cell Rate: 0 cell/sec

Maximum Burst Size: 0 cell

The following table describes the labels in this screen.

Table 14 WAN > More Connections > Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyXEL Device will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	This field is enabled if **RIP Direction** is not **None**. The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Select **None** to disable it.
ATM QoS	
ATM QoS Type	Select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR-nRT** (Variable Bit Rate-non Real Time) or **VBR-RT** (Variable Bit Rate-Real Time) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.

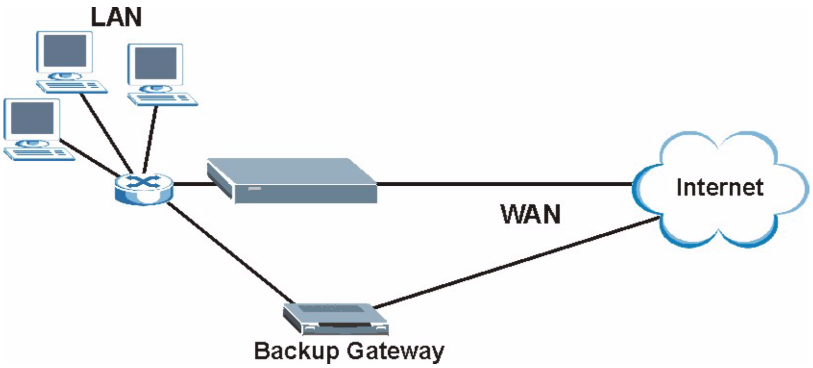
Table 14 WAN > More Connections > Advanced Setup (continued)

LABEL	DESCRIPTION
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

5.6 Traffic Redirect

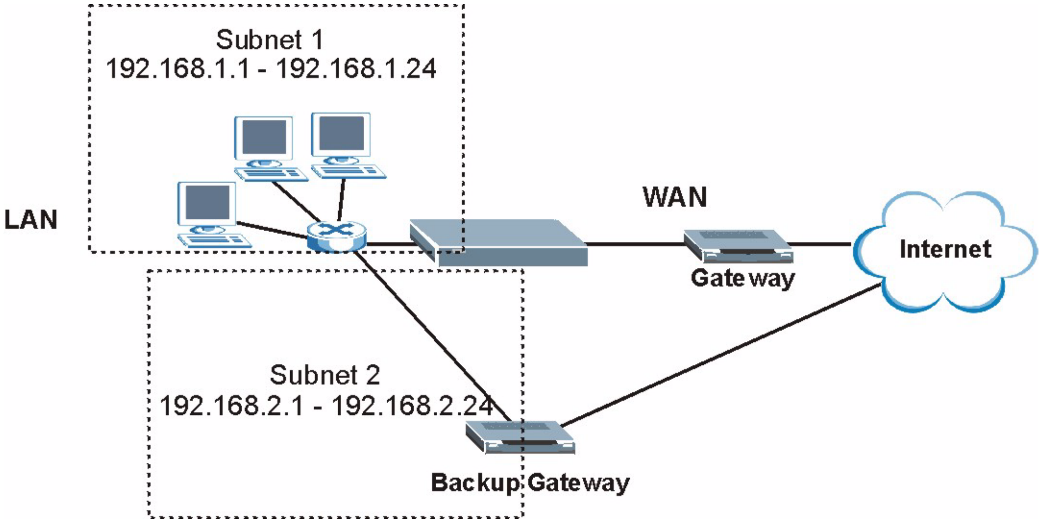
Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet. An example is shown in the figure below.

Figure 28 Traffic Redirect Example



The following network topology allows you to avoid triangle route security issues when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the ZyXEL Device itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure filters that allow packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

Figure 29 Traffic Redirect LAN Setup



5.7 Dial Backup Interface

The **Dial Backup** port can be used in reserve, as a traditional dial-up connection should the broadband connection to the WAN port fail. To set up the auxiliary port (**Dial Backup**) for use in the event that the regular WAN connection is dropped, first make sure you have set up the switch and port connection. See Section 5.8 on page 75 for more information.

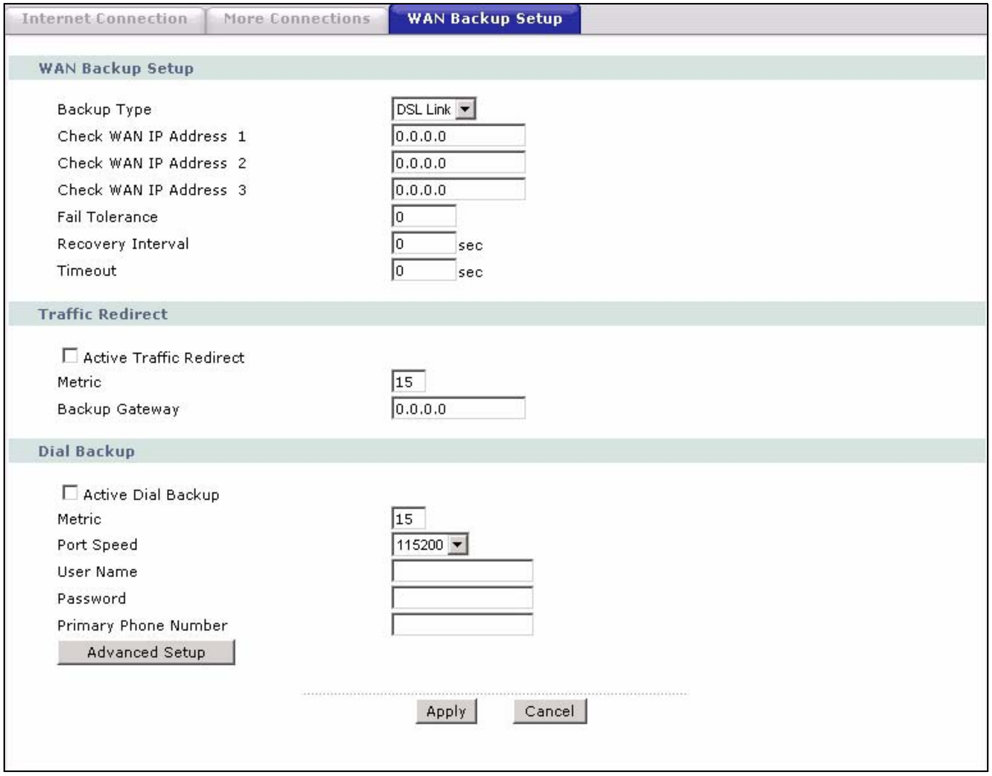
5.8 CON/AUX Port for Dial Backup

Use the CON/AUX port to configure the ZyXEL Device for Dial Backup via a modem. Set the CON/AUX switch of the ZyXEL Device to AUX (Auxiliary) side to use the CON/AUX port as a backup port for Internet access via a modem. Connect the RJ-45 connector of the console cable to the CON/AUX port of the ZyXEL Device and the other end to a serial port (COM1, COM2 or other COM port) on your modem.

5.9 Configuring WAN Backup Setup

Use this screen to forward traffic to a backup gateway or to use the dial-backup port when the ZyXEL Device cannot connect to the Internet. To open this screen, click **WAN** > **WAN Backup Setup**. The screen appears as shown.

Figure 30 WAN > WAN Backup Setup



WAN Backup Setup

Backup Type	DSL Link
Check WAN IP Address 1	0.0.0.0
Check WAN IP Address 2	0.0.0.0
Check WAN IP Address 3	0.0.0.0
Fail Tolerance	0
Recovery Interval	0 sec
Timeout	0 sec

Traffic Redirect

☐ Active Traffic Redirect	
Metric	15
Backup Gateway	0.0.0.0

Dial Backup

☐ Active Dial Backup	
Metric	15
Port Speed	115200
User Name	
Password	
Primary Phone Number	

The following table describes the labels in this screen.

Table 15 WAN > WAN Backup Setup

LABEL	DESCRIPTION
Backup Type	Select the method that the ZyXEL Device uses to check the DSL connection. Select **DSL Link** to have the ZyXEL Device check if the connection to the DSLAM is up. Select **ICMP** to have the ZyXEL Device periodically ping the IP addresses configured in the **Check WAN IP Address** fields.
Check WAN IP Address 1-3	Configure this field to test your ZyXEL Device's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). Note: If you activate either traffic redirect or dial backup, you must configure at least one IP address here. When using a WAN backup connection, the ZyXEL Device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Fail Tolerance	Type the number of times (2 recommended) that your ZyXEL Device pings the IP addresses configured in the **Check WAN IP Address** field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval	When the ZyXEL Device is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the ZyXEL Device to wait between checks. Allow more time if your destination IP address handles lots of traffic.
Timeout	Type the number of seconds (3 recommended) for your ZyXEL Device to wait for a ping response from one of the IP addresses in the **Check WAN IP Address** field before timing out the request. The WAN connection is considered "down" after the ZyXEL Device times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	Traffic redirect forwards traffic to a backup gateway when the ZyXEL Device cannot connect to the Internet.
Active Traffic Redirect	Select this check box to have the ZyXEL Device use traffic redirect if the normal WAN connection goes down. Note: If you activate traffic redirect, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL Device automatically forwards traffic to this IP address if the ZyXEL Device's Internet connection terminates.
Dial Backup	

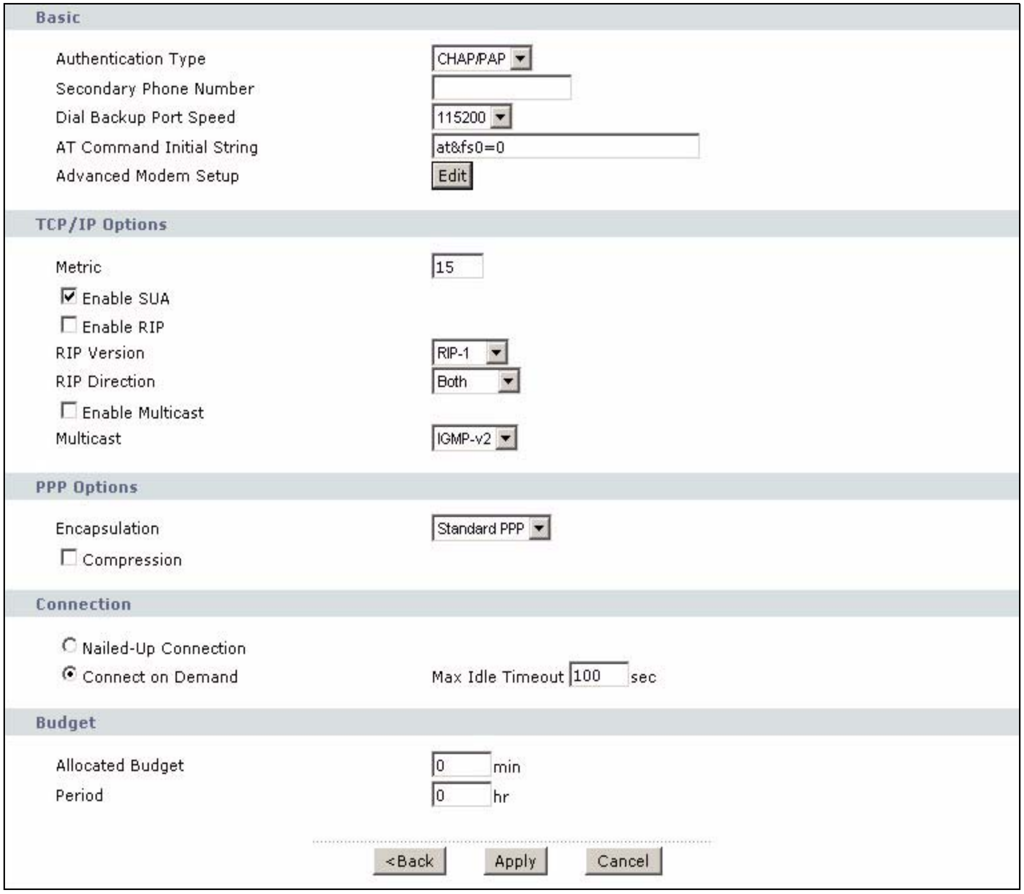
Table 15 WAN > WAN Backup Setup (continued)

LABEL	DESCRIPTION
Active Dial Backup	Select this to have the ZyXEL Device use a dial-backup connection if the normal WAN connection goes down. Note: If you activate dial backup, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Port Speed	Use the drop-down list box to select the speed of the connection between the DSL port and the external device.
User Name	Type the login name assigned by your ISP.
Password	Type the password assigned by your ISP.
Primary Phone Number	Type the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your ZyWALL dials the Secondary Phone number, if available. (See **Advanced Setup**.) Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Advanced Setup	Click this to configure advanced settings for the dial-backup connection.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

5.9.1 Advanced Backup Setup

Use this screen to change your ZyXEL Device’s advanced dial backup settings. Click **WAN** > **WAN Backup Setup > Advanced Setup**. The screen appears as shown.

Figure 31 WAN > WAN Backup Setup > Advanced Setup



Basic

Authentication Type: CHAP/PAP

Secondary Phone Number:

Dial Backup Port Speed: 115200

AT Command Initial String: at&fs0=0

Advanced Modem Setup: Edit

TCP/IP Options

Metric: 15

☑ Enable SUA

□ Enable RIP

RIP Version: RIP-1

RIP Direction: Both

□ Enable Multicast

Multicast: IGMP-v2

PPP Options

Encapsulation: Standard PPP

□ Compression

Connection

○ Nailed-Up Connection

● Connect on Demand — Max Idle Timeout 100 sec

Budget

Allocated Budget: 0 min

Period: 0 hr

The following table describes the labels in this screen.

Table 16 WAN > WAN Backup Setup > Advanced Setup

LABEL	DESCRIPTION
Basic	
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your ZyXEL Device accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your ZyXEL Device accepts CHAP only. **PAP** - Your ZyXEL Device accepts PAP only.
Secondary Phone Number	Type the backup phone number from the ISP. If the Primary Phone number is busy or does not answer, your ZyWALL dials the Secondary Phone number, if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Dial Backup Port Speed	Select the speed of the connection between the Dial Backup port and the external device. Available speeds are **9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps.
AT Command Initial String	Enter the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.
Advanced Modem Setup	Click **Edit** to change the advanced settings for the modem.
TCP/IP Options	

Table 16 WAN > WAN Backup Setup > Advanced Setup (continued)

LABEL	DESCRIPTION
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Enable SUA	Select this if you have one public IP address and want to use NAT, or clear it to disable NAT.
Enable RIP	Select this if you want to enable RIP in the dial-backup connection. RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. Clear this if you want the ZyXEL Deviceto not send any RIP packets and to ignore any RIP packets received.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.
RIP Direction	The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**. When set to **Both** or **Out Only**, the ZyXEL Device will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives.
Enable Multicast	Select this if you want to enable IGMP in the dial-backup connection. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group.
Multicast	The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**.
PPP Options	
Encapsulation	Select **CISCO PPP** from the drop-down list box if your dial backup WAN device uses Cisco PPP encapsulation, otherwise select **Standard PPP**.
Compression	Select this to turn on stac compression.
Connection	
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The ZyXEL Device will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
Budget	
Allocated Budget	Enter the maximum amount of time (in minutes) each call can last. Enter 0 if there is no limit. With **Period**, you can set a limit on the total outgoing call time of the ZyXEL Device within a certain period of time. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.
Period	Enter how often (in hours) the **Allocated Budget** is reset. For example, if you can call for thirty minutes every hour, set the **Allocated Budget** to 30, and set this field to 1.

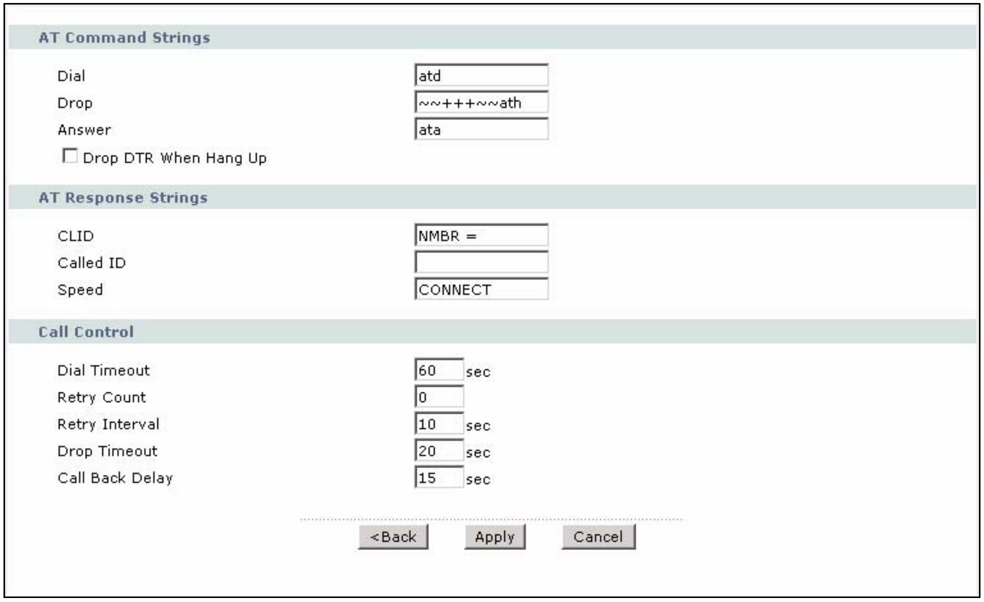
Table 16 WAN > WAN Backup Setup > Advanced Setup (continued)

LABEL	DESCRIPTION
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

5.9.2 Advanced Modem Settings for Dial Backup

Use this screen to change your ZyXEL Device's modem settings for dial backup. Click **WAN** > **WAN Backup Setup** > **Advanced Setup** > **Edit**. The screen appears as shown.

Figure 32 WAN > WAN Backup Setup > Advanced Setup > Edit



AT Command Strings

Dial	atd
Drop	~~+++~~ath
Answer	ata

□ Drop DTR When Hang Up

AT Response Strings

CLID	NMBR =
Called ID	
Speed	CONNECT

Call Control

Dial Timeout	60 sec
Retry Count	0
Retry Interval	10 sec
Drop Timeout	20 sec
Call Back Delay	15 sec

The following table describes the labels in this screen.

Table 17 WAN > WAN Backup Setup > Advanced Setup > Edit

LABEL	DESCRIPTION
AT Command Strings	
Dial	Enter the AT Command string to make a call.
Drop	Enter the AT Command string to drop a call. "~" represents a one second wait, for example "~~~+++~~ath" can be used if your modem has a slow response time.
Answer	Enter the AT Command string to answer a call.
Drop DTR When Hang Up	Select this if you want the DTR (Data Terminal Ready) signal to be dropped after the **Drop** string is sent out.
AT Response Strings	
CLID	Enter the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyXEL Device capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.
Called ID	Enter the keyword preceding the dialed number.
Speed	Enter the keyword preceding the connection speed.

Table 17 WAN > WAN Backup Setup > Advanced Setup > Edit (continued)

LABEL	DESCRIPTION
Call Control	
Dial Timeout	Enter a number of seconds for the ZyXEL Device to keep trying to set up an outgoing call before timing out (stopping). The ZyXEL Device times out and stops if it cannot set up an outgoing call within the timeout value.
Retry Count	Enter a number of times for the ZyXEL Device to retry a busy or no-answer phone number before blacklisting the number.
Retry Interval	Enter a number of seconds for the ZyXEL Device to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.
Drop Timeout	Enter a number of seconds for the ZyXEL Device to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.
Call Back Delay	Enter a number of seconds for the ZyXEL Device to wait between dropping a callback request call and dialing the corresponding callback call.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6

LAN Setup

This chapter describes how to configure LAN settings.

6.1 LAN Overview

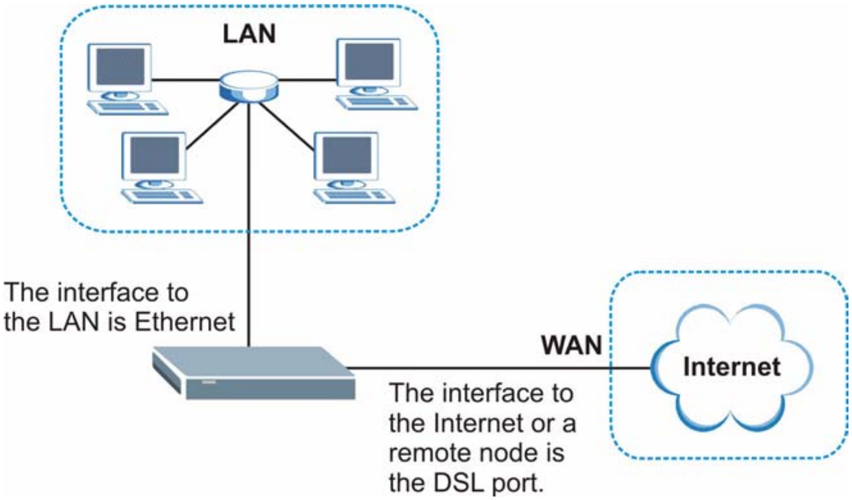
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See Section 6.3 on page 87 to configure the **LAN** screens.

6.1.1 LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the ZyXEL Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 33 LAN and WAN IP Addresses


LAN
The interface to the LAN is Ethernet
WAN
Internet
The interface to the Internet or a remote node is the DSL port.

6.1.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

6.1.2.1 IP Pool Setup

The ZyXEL Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

6.1.3 DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP gives you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**, otherwise, leave them blank.

Some ISP’s choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The ZyXEL Device supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields in the **DHCP Setup** screen are not specified, for instance, left as **0.0.0.0**, the ZyXEL Device tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **DHCP Setup** screen. This way, the ZyXEL Device can pass the DNS servers to the computers and the computers can query the DNS server directly without the ZyXEL Device’s intervention.

6.1.4 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in the **DHCP Setup** screen.
- The ZyXEL Device acts as a DNS proxy when the **Primary** and **Secondary DNS Server** fields are left as **0.0.0.0** in the **DHCP Setup** screen.

6.2 LAN TCP/IP

The ZyXEL Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

The LAN parameters of the ZyXEL Device are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

6.2.1 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyXEL Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyXEL Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

6.2.1.1 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

6.2.2 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both -** the ZyXEL Device will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only -** the ZyXEL Device will not send any RIP packets but will accept all RIP packets received.
- **Out Only -** the ZyXEL Device will send out RIP packets but will not accept any RIP packets received.
- **None -** the ZyXEL Device will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

6.2.3 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

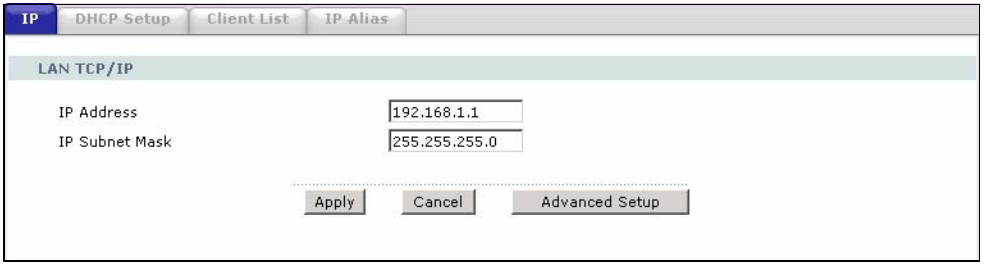
IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information. IP multicasting can be enabled/disabled on the ZyXEL Device LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

6.3 Configuring LAN IP

Use this screen to set the LAN IP address of your ZyXEL Device. Click **LAN** > **IP**. See Section 6.1 on page 83 for background information.

Figure 34 LAN > IP



LAN TCP/IP

IP Address 192.168.1.1

IP Subnet Mask 255.255.255.0

The following table describes the fields in this screen.

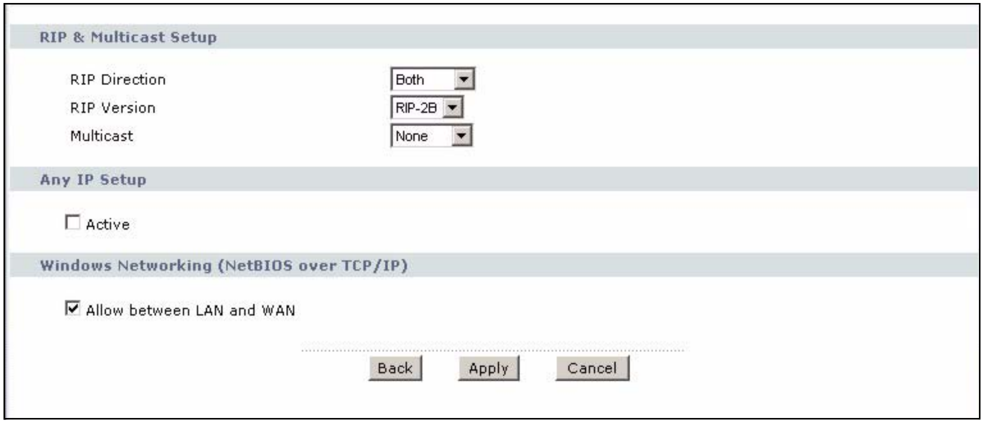
Table 18 LAN > IP

LABEL	DESCRIPTION
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask for your network. See Section 6.2.1 on page 85 for more information.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Advanced Setup	Click this button to display the **Advanced LAN Setup** screen and edit more details of your LAN setup.

6.3.1 Configuring Advanced LAN Setup

Use this screen to edit your ZyXEL Device's advanced LAN settings. Click the **Advanced Setup** button in the **LAN IP** screen. The screen appears as shown.

Figure 35 LAN > IP > Advanced Setup



RIP & Multicast Setup

RIP Direction: Both

RIP Version: RIP-2B

Multicast: None

Any IP Setup

□ Active

Windows Networking (NetBIOS over TCP/IP)

☑ Allow between LAN and WAN

The following table describes the labels in this screen.

Table 19 LAN > IP > Advanced Setup

LABEL	DESCRIPTION
RIP & Multicast Setup	
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyXEL Device will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	This field is enabled if **RIP Direction** is not **None**. The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Select **None** to disable it.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Back	Click **Back** to return to the previous screen.

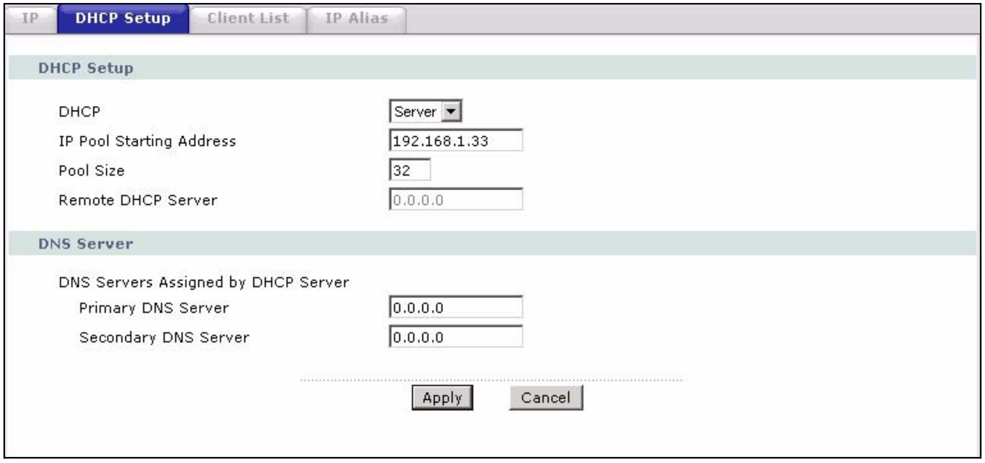
Table 19 LAN > IP > Advanced Setup (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.4 DHCP Setup

Use this screen to configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN.

Figure 36 LAN > DHCP Setup



DHCP Setup

DHCP: Server

IP Pool Starting Address: 192.168.1.33

Pool Size: 32

Remote DHCP Server: 0.0.0.0

DNS Server

DNS Servers Assigned by DHCP Server

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

The following table describes the labels in this screen.

Table 20 LAN > DHCP Setup

LABEL	DESCRIPTION
DHCP Setup	
DHCP	Select what type of DHCP services the ZyXEL Device provides to the network. Choices are: **None** - the ZyXEL Device does not provide any DHCP services. There is already a DHCP server on the network. **Relay** - the ZyXEL Device routes DHCP requests to the DHCP server. There may be a DHCP server on another network. **Server** - the ZyXEL Device assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyXEL Device is the DHCP server for the network.
IP Pool Starting Address	This field is enabled if the ZyXEL Device is a **Server**. Enter the first of the contiguous addresses in the IP address pool.
Pool Size	This field is enabled if the ZyXEL Device is a **Server**. Enter the size of, or the number of addresses in, the IP address pool.
Remote DHCP Server	This field is enabled if the ZyXEL Device is a **Relay**. Enter the IP address of the DHCP server to which the ZyXEL Device should route requests.
DNS Server	
DNS Servers Assigned by DHCP Server	The ZyXEL Device passes a DNS (Domain Name System) server IP address to the DHCP clients.

Table 20 LAN > DHCP Setup (continued)

LABEL	DESCRIPTION
Primary DNS Server Secondary DNS Server	This field is not available when you set **DHCP** to **Relay**. Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask. If the fields are left as 0.0.0.0, the ZyXEL Device acts as a DNS proxy and forwards the DHCP client's DNS query to the real DNS server learned through IPCP and relays the response back to the computer.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

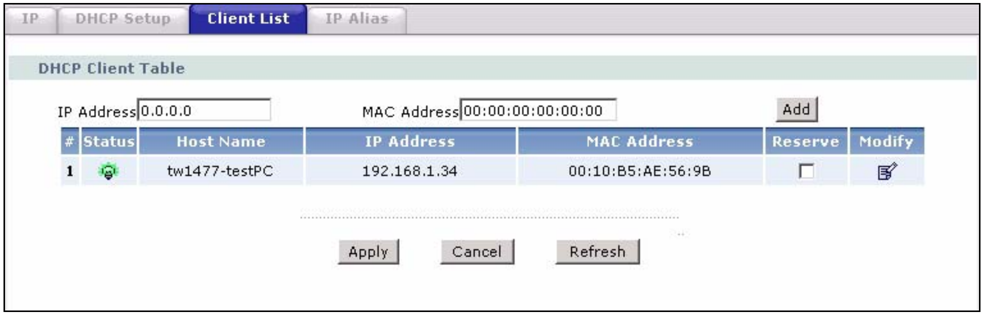
6.5 LAN Client List

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Use this screen to change your ZyXEL Device's static DHCP settings. Click **Network > LAN > Client List**. The screen appears as shown.

Figure 37 LAN > Client List



DHCP Client Table

IP Address 0.0.0.0

MAC Address 00:00:00:00:00:00

#	Status	Host Name	IP Address	MAC Address	Reserve	Modify
1	●	tw1477-testPC	192.168.1.34	00:10:B5:AE:56:9B	□	✎

The following table describes the labels in this screen.

Table 21 LAN > Client List

LABEL	DESCRIPTION
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address specified below. The IP address should be within the range of IP addresses you specified in the **DHCP Setup** for the DHCP client.
MAC Address	Enter the MAC address of a computer on your LAN.
Add	Click **Add** to add a static DHCP entry.
#	This is the index number of the static IP table entry (row).
Status	This field displays whether the client is connected to the ZyXEL Device.
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.

Table 21 LAN > Client List (continued)

LABEL	DESCRIPTION
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select the check box(es) in each entry to have the ZyXEL Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 32 entries in this table.
Modify	Click the modify icon to have the IP address field editable and change it.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Refresh	Click **Refresh** to reload the DHCP table.

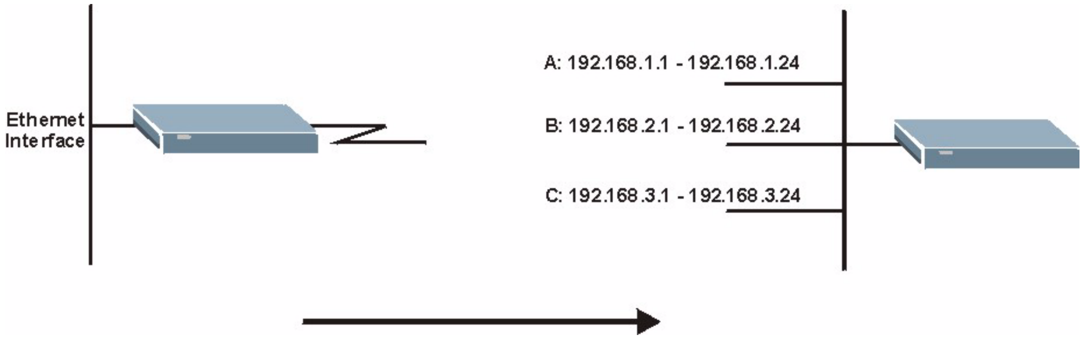
6.6 LAN IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network.

Make sure that the subnets of the logical networks do not overlap.

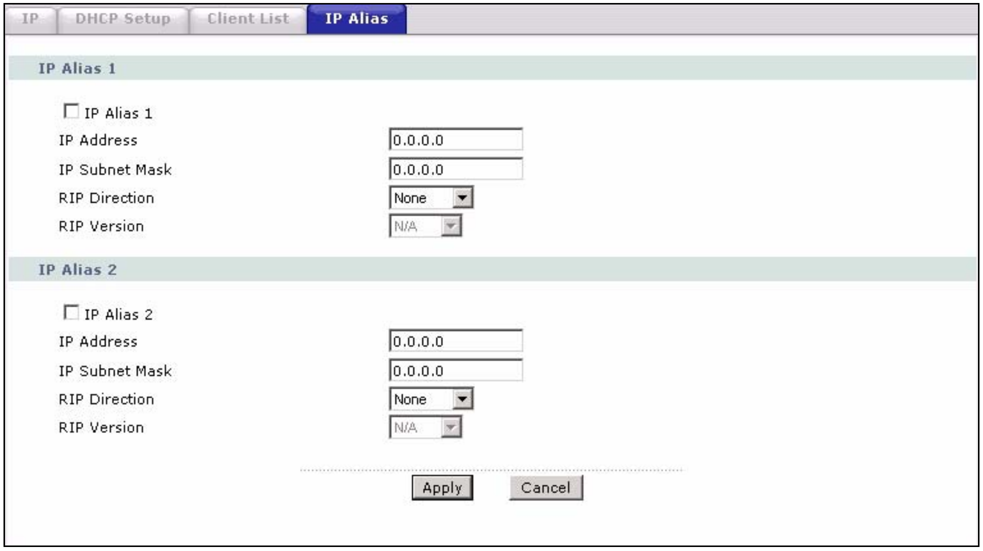
The following figure shows a LAN divided into subnets A, B, and C.

Figure 38 Physical Network & Partitioned Logical Networks


Ethernet Interface
A: 192.168.1.1 - 192.168.1.24
B: 192.168.2.1 - 192.168.2.24
C: 192.168.3.1 - 192.168.3.24

Use this screen to configure subnets on the LAN. Click **Network** > **LAN** > **IP Alias**. The screen appears as shown.

Figure 39 LAN > IP Alias



IP Alias 1

☐ IP Alias 1

IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
RIP Direction	None
RIP Version	N/A

IP Alias 2

☐ IP Alias 2

IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
RIP Direction	None
RIP Version	N/A

The following table describes the labels in this screen.

Table 22 LAN > IP Alias

LABEL	DESCRIPTION
IP Alias 1, 2	Select the check box to configure another LAN network for the ZyXEL Device.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyXEL Device will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	This field is enabled if **RIP Direction** is not **None**. The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyXEL Device sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

7

Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the ZyXEL Device.

7.1 NAT Overview

NAT (Network Address Translation, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

7.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 23 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

7.1.2 What NAT Does

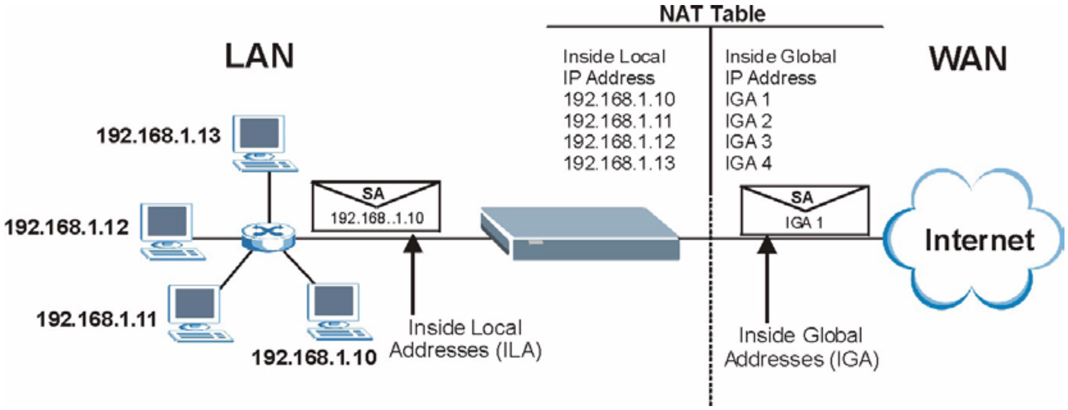
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see Table 24 on page 96), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

7.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyXEL Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 40 How NAT Works

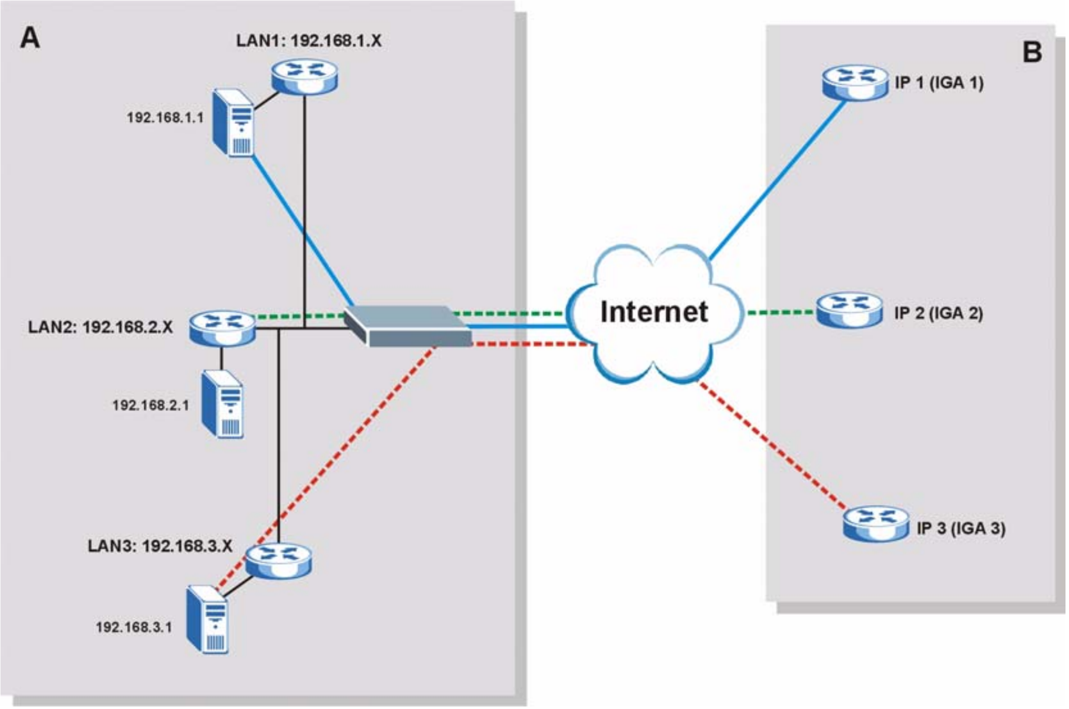


Inside Local IP Address	Inside Global IP Address
192.168.1.10	IGA 1
192.168.1.11	IGA 2
192.168.1.12	IGA 3
192.168.1.13	IGA 4

7.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyXEL Device can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

Figure 41 NAT Application With IP Alias



7.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the ZyXEL Device maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the ZyXEL Device maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
- **Many to Many Overload**: In Many-to-Many Overload mode, the ZyXEL Device maps the multiple local IP addresses to shared global IP addresses.
- **Many-to-Many No Overload**: In Many-to-Many No Overload mode, the ZyXEL Device maps each local IP address to a unique global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do NOT change for **One-to-One** and **Many-to-Many No Overload** NAT mapping types.

The following table summarizes these types.

Table 24 NAT Mapping Types

TYPE	IP MAPPING
One-to-One	ILA1←→ IGA1

Many-to-One (SUA/PAT)	ILA1←→ IGA1
	ILA2←→ IGA1
	…

Many-to-Many Overload	ILA1←→ IGA1
	ILA2←→ IGA2
	ILA3←→ IGA1
	ILA4←→ IGA2
	…

Many-to-Many No Overload	ILA1←→ IGA1
	ILA2←→ IGA2
	ILA3←→ IGA3
	…

Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1

7.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyXEL Device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in Table 24 on page 96.

- Choose **SUA Only** if you have just one public WAN IP address for your ZyXEL Device.
- Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyXEL Device.

7.2.1 SIP ALG

Some applications, such as SIP, cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload.

Some NAT routers may include a SIP Application Layer Gateway (ALG). An Application Layer Gateway (ALG) manages a specific protocol (such as SIP, H.323 or FTP) at the application layer.

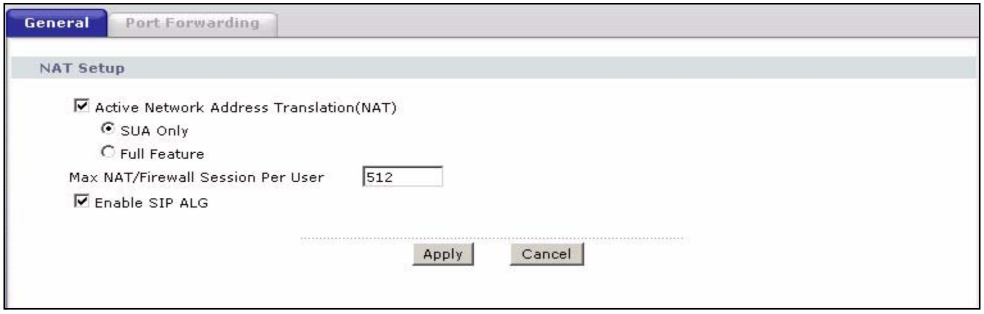
A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream.

When the ZyXEL Device registers with the SIP register server, the SIP ALG translates the ZyXEL Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your ZyXEL Device is behind a SIP ALG.

7.3 NAT General Setup

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyXEL Device. Click **Network > NAT** to open the following screen.

Figure 42 NAT > General



☑ Active Network Address Translation(NAT)

● SUA Only

○ Full Feature

Max NAT/Firewall Session Per User 512

☑ Enable SIP ALG

The following table describes the labels in this screen.

Table 25 NAT General

LABEL	DESCRIPTION
Active Network Address Translation (NAT)	Select this check box to enable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your ZyXEL Device.
Full Feature	Select this radio button if you have multiple public WAN IP addresses for your ZyXEL Device.
Max NAT/ Firewall Session Per User	When computers use peer to peer applications, such as file sharing applications, they need to establish NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet. If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using all of the available NAT sessions.
Enable SIP ALG	Select this to make sure SIP (VoIP) works correctly with port-forwarding and port-triggering rules.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

7.4 Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

7.4.1 Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

7.4.2 Port Forwarding: Services and Port Numbers

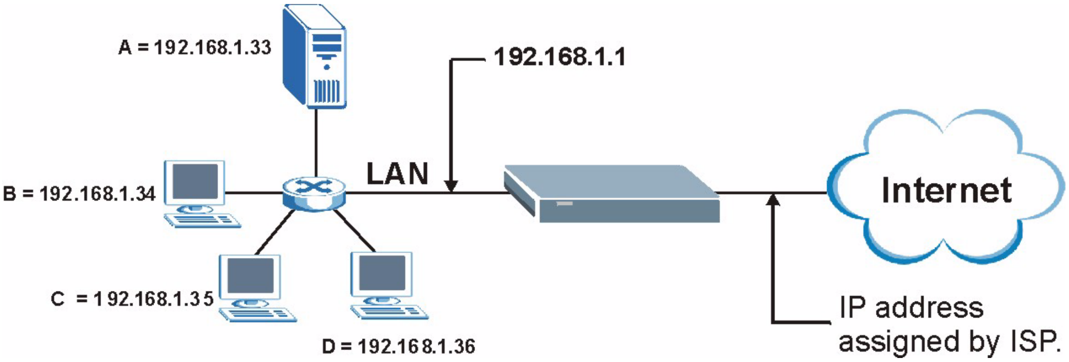
Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

The most often used port numbers are shown in Appendix F on page 321. Please refer to RFC 1700 for further information about port numbers.

7.4.3 Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 43 Multiple Servers Behind NAT Example



7.5 Configuring Port Forwarding

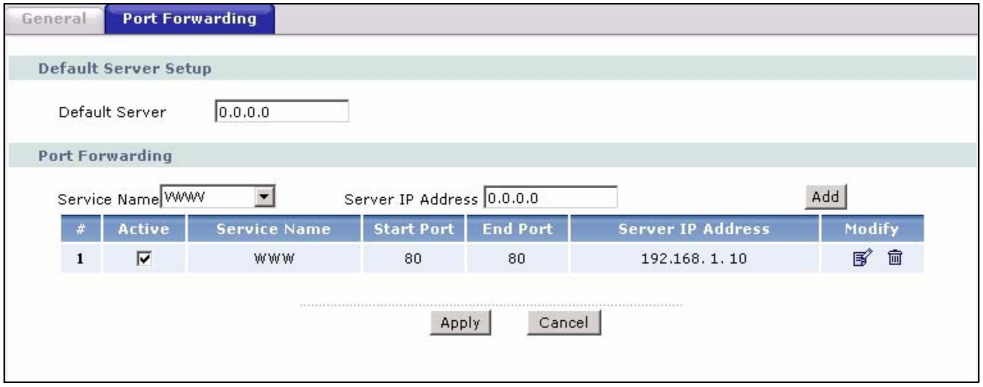
The **Port Forwarding** screen is available when you select **SUA Only** in the **NAT > General** screen or when you edit a server mapping set with **Full Feature** NAT.

If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

Click **Network** > **NAT** > **Port Forwarding** to open the following screen.

See Appendix F on page 321 for port numbers commonly used for particular services.

Figure 44 NAT > Port Forwarding



Default Server Setup

Default Server: 0.0.0.0

Port Forwarding

Service Name: WWW Server IP Address: 0.0.0.0

#	Active	Service Name	Start Port	End Port	Server IP Address	Modify
1	☑	WWW	80	80	192.168. 1. 10	

The following table describes the fields in this screen.

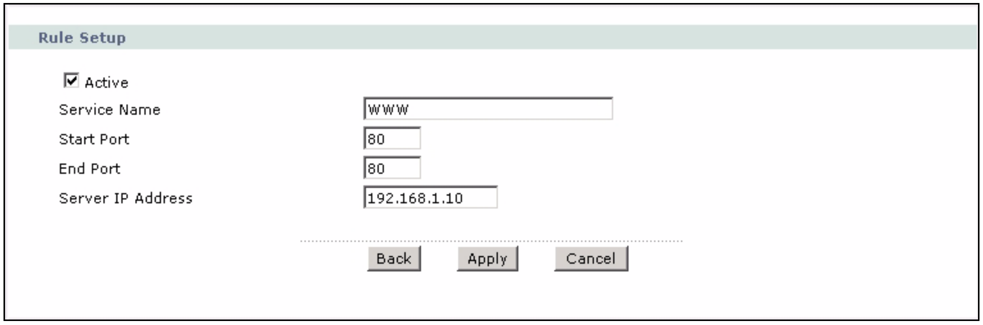
Table 26 NAT > Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.
Port Forwarding	
Service Name	Select a service from the drop-down list box or select **User define** to go to the **Rule Setup** screen and define your own service and its forwarding actions.
Server IP Address	Enter the IP address of the server for the specified service.
Add	Click this button to add a rule to the table below.
#	This is the rule index number (read-only).
Active	Click this check box to enable the rule.
Service Name	This is a service's name.
Start Port	This is the first port number that identifies a service.
End Port	This is the last port number that identifies a service.
Server IP Address	This is the server's IP address.
Modify	Click the edit icon to go to the screen where you can edit the port forwarding rule. Click the delete icon to delete an existing port forwarding rule. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to return to the previous configuration.

7.5.1 Port Forwarding Rule Edit

Use this screen to edit a port forwarding rule. Click the rule's edit icon in the **Port Forwarding** screen to display the screen shown next.

Figure 45 NAT > Port Forwarding > Edit



Rule Setup

☑ Active

Service Name: www

Start Port: 80

End Port: 80

Server IP Address: 192.168.1.10

The following table describes the fields in this screen.

Table 27 NAT > Port Forwarding > Edit

LABEL	DESCRIPTION
Active	Click this check box to enable the rule.
Service Name	Enter a name to identify this port-forwarding rule.
Start Port	Enter a port number in this field. To forward only one port, enter the port number again in the **End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port** field.
End Port	Enter a port number in this field. To forward only one port, enter the port number again in the **Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port** field above.
Server IP Address	Enter the inside IP address of the server here.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

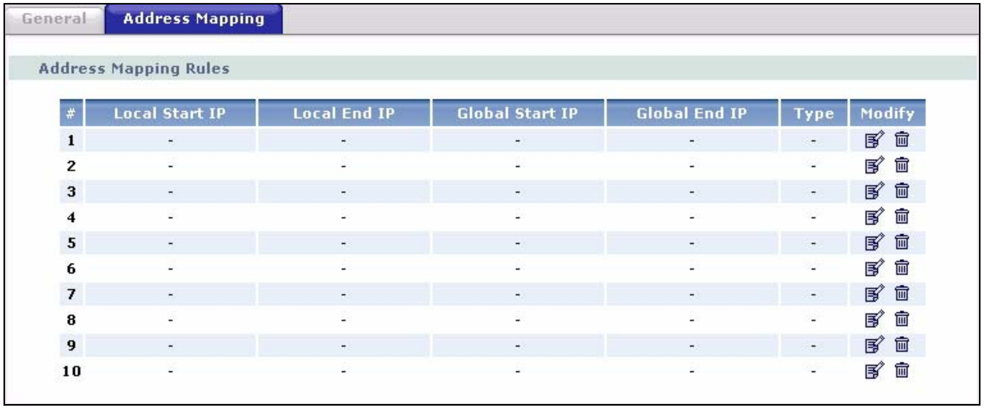
7.6 Address Mapping

The **Address Mapping** screen is available only when you select **Full Feature** in the **NAT > General** screen.

Ordering your rules is important because the ZyXEL Device applies the rules in the order that you specify. When a rule matches the current packet, the ZyXEL Device takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

Use this screen to change your ZyXEL Device’s address mapping settings. Click **Network > NAT > Address Mapping** to open the following screen.

Figure 46 NAT > Address Mapping



Address Mapping Rules

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	-	-	-	-	-	✎ 🗑
2	-	-	-	-	-	✎ 🗑
3	-	-	-	-	-	✎ 🗑
4	-	-	-	-	-	✎ 🗑
5	-	-	-	-	-	✎ 🗑
6	-	-	-	-	-	✎ 🗑
7	-	-	-	-	-	✎ 🗑
8	-	-	-	-	-	✎ 🗑
9	-	-	-	-	-	✎ 🗑
10	-	-	-	-	-	✎ 🗑

The following table describes the fields in this screen.

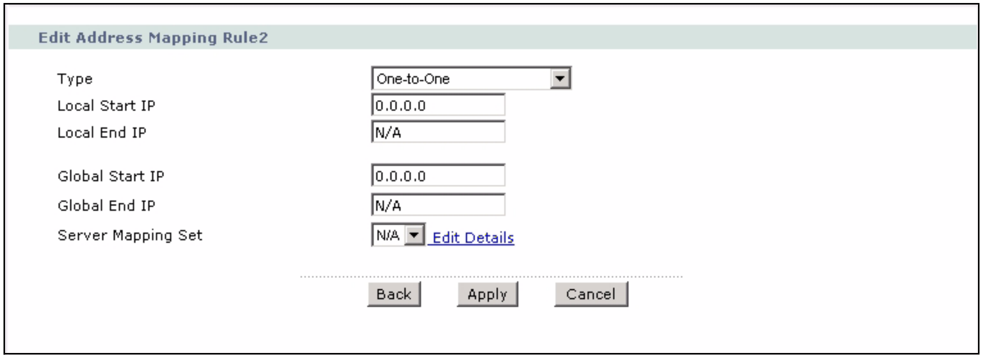
Table 28 NAT > Address Mapping

LABEL	DESCRIPTION
#	This is the rule index number.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-one** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-one**, **Many-to-One** and **Server** mapping types.
Type	**1-1**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **M-1**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (in other words PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. **M-M Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. **MM No** (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Modify	Click the edit icon to go to the screen where you can edit the address mapping rule. Click the delete icon to delete an existing address mapping rule. Note that subsequent rules move up by one when you take this action.

7.6.1 Address Mapping Rule Edit

Use this screen to edit an address mapping rule. Click the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

Figure 47 NAT > Address Mapping > Edit



Edit Address Mapping Rule2

Type	One-to-One
Local Start IP	0.0.0.0
Local End IP	N/A
Global Start IP	0.0.0.0
Global End IP	N/A
Server Mapping Set	N/A Edit Details

The following table describes the fields in this screen.

Table 29 NAT > Address Mapping > Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. **One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (in other words PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. **Many-to-Many No Overload**: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Server Mapping Set	Only available when **Type** is set to **Server**. Select a number from the drop-down menu to choose a server mapping set.
Edit Details	Click this link to go to the **Port Forwarding** screen (Section 7.5 on page 99) to edit the server mapping set that you have selected in the **Server Mapping Set** field.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

PART III
Security

Filter

This chapter shows how to configure Internet security filters on your ZyXEL Device.

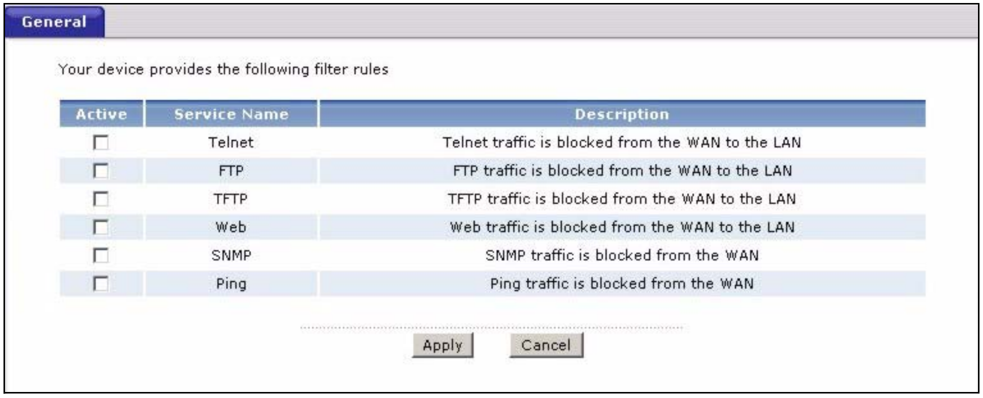
8.1 Configuring Filter

The ZyXEL Device can use predefined filters to stop packets of specified types from passing from the WAN to the LAN.

If you want to enable remote management of the ZyXEL Device from the WAN, ensure that the settings in this screen allow packets of the relevant type to pass from the WAN.

Click **Security** > **Filter** in the navigation panel to open the following screen.

Figure 48 Security > Filter



Your device provides the following filter rules

Active	Service Name	Description
□	Telnet	Telnet traffic is blocked from the WAN to the LAN
□	FTP	FTP traffic is blocked from the WAN to the LAN
□	TFTP	TFTP traffic is blocked from the WAN to the LAN
□	Web	Web traffic is blocked from the WAN to the LAN
□	SNMP	SNMP traffic is blocked from the WAN
□	Ping	Ping traffic is blocked from the WAN

The following table describes the labels in this screen.

Table 30 Internet Security

LABEL	DESCRIPTION
Telnet	Select this to stop all telnet packets passing from the WAN to the LAN. Telnet traffic from the LAN can still pass through to the WAN.
FTP	Select this to stop all FTP traffic passing from the WAN to the LAN. FTP traffic from the LAN can still pass through to the WAN.
TFTP	Select this to stop all TFTP traffic passing from the WAN to the LAN. TFTP traffic from the LAN can still pass through to the WAN.

Table 30 Internet Security

LABEL	DESCRIPTION
Web	Select this to stop all HTTP traffic passing from the WAN to the LAN.
SNMP	Select this to stop all SNMP traffic passing from the WAN to the ZyXEL Device. SNMP traffic from the LAN can still access the ZyXEL Device.
Ping	Select this to stop all ICMP Echo traffic passing from the WAN to the LAN.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

PART IV
Advanced Setup

9

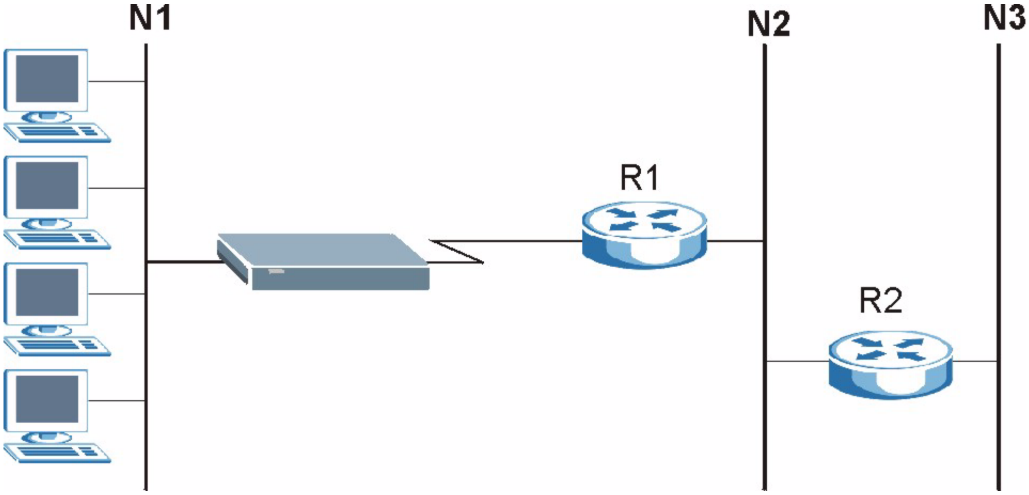
Static Route

This chapter shows you how to configure static routes for your ZyXEL Device.

9.1 Static Route

Each remote node specifies only the network to which the gateway is directly connected, and the ZyXEL Device has no knowledge of the networks beyond. For instance, the ZyXEL Device knows about network N2 in the following figure through remote node Router 1. However, the ZyXEL Device is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the ZyXEL Device about the networks beyond the remote nodes.

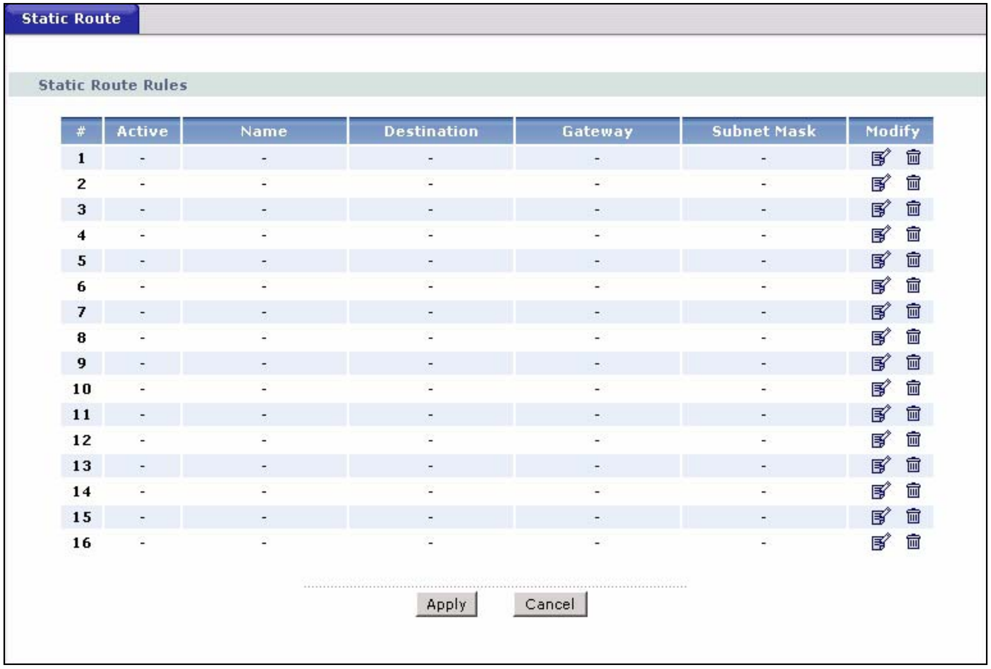
Figure 49 Example of Static Routing Topology



9.2 Configuring Static Route

Use this screen to look at static routes in the ZyXEL Device. Click **Advanced** > **Static Route** to open the **Static Route** screen.

Figure 50 Static Route > Static Route



#	Active	Name	Destination	Gateway	Subnet Mask	Modify
1	-	-	-	-	-	✎ 🗑
2	-	-	-	-	-	✎ 🗑
3	-	-	-	-	-	✎ 🗑
4	-	-	-	-	-	✎ 🗑
5	-	-	-	-	-	✎ 🗑
6	-	-	-	-	-	✎ 🗑
7	-	-	-	-	-	✎ 🗑
8	-	-	-	-	-	✎ 🗑
9	-	-	-	-	-	✎ 🗑
10	-	-	-	-	-	✎ 🗑
11	-	-	-	-	-	✎ 🗑
12	-	-	-	-	-	✎ 🗑
13	-	-	-	-	-	✎ 🗑
14	-	-	-	-	-	✎ 🗑
15	-	-	-	-	-	✎ 🗑
16	-	-	-	-	-	✎ 🗑

The following table describes the labels in this screen.

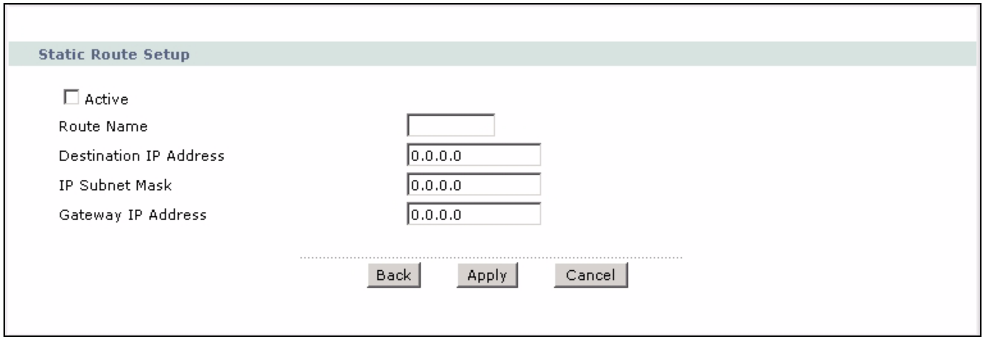
Table 31 Static Route > Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Active	This field shows whether this static route is active (**Yes**) or not (**No**).
Name	This is the name that describes or identifies this route.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Subnet Mask	This is the subnet mask of the static route.
Modify	Click the edit icon to go to the screen where you can set up a static route on the ZyXEL Device. Click the delete icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.2.1 Static Route Edit

Select a static route index number and click **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 51 Static Route > Static Route > Edit



Static Route Setup

☐ Active

Route Name	
Destination IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0

The following table describes the labels in this screen.

Table 32 Static Route > Static Route > Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Back	Click **Back** to return to the previous screen without saving.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10

Dynamic DNS Setup

This chapter discusses how to configure your ZyXEL Device to use Dynamic DNS.

10.1 Dynamic DNS Overview

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

10.1.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

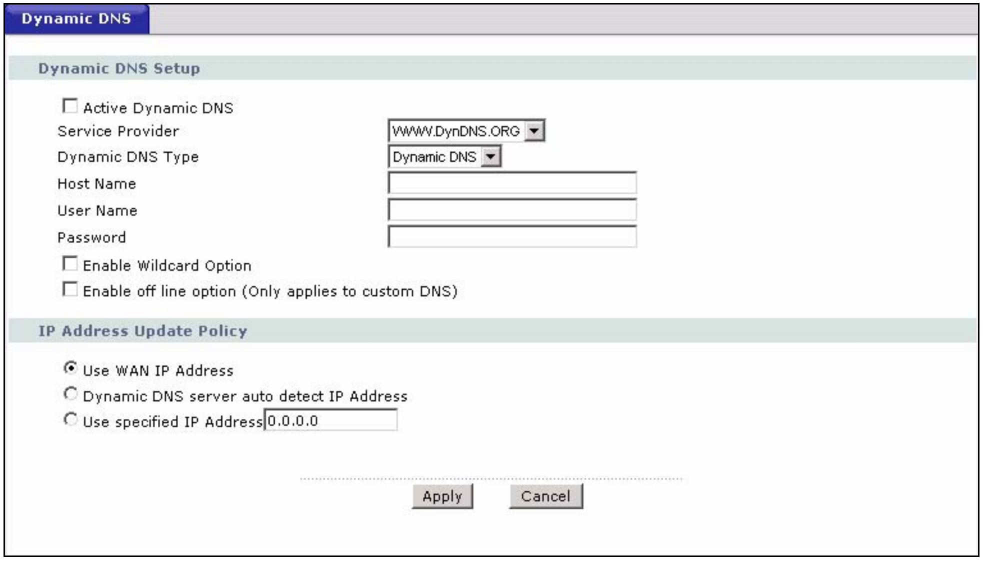
See Section 10.2 on page 115 for configuration instruction.

10.2 Configuring Dynamic DNS

Use this screen to change your ZyXEL Device’s DDNS settings. Click **Advanced** > **Dynamic DNS**. The screen appears as shown.

See Section 10.1 on page 115 for more information.

Figure 52 Dynamic DNS > Dynamic DNS



Dynamic DNS Setup

□ Active Dynamic DNS

Service Provider: WWW.DynDNS.ORG

Dynamic DNS Type: Dynamic DNS

Host Name:

User Name:

Password:

□ Enable Wildcard Option

□ Enable off line option (Only applies to custom DNS)

IP Address Update Policy

● Use WAN IP Address

○ Dynamic DNS server auto detect IP Address

○ Use specified IP Address 0.0.0.0

The following table describes the fields in this screen.

Table 33 Dynamic DNS > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Active Dynamic DNS	Select this to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
User Name	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when **Custom DNS** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.
Dynamic DNS server auto detect IP Address	Select this option only when there are one or more NAT routers between the ZyXEL Device and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyXEL Device and the DDNS server.

Table 33 Dynamic DNS > Dynamic DNS (continued)

LABEL	DESCRIPTION
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11

Remote Management Configuration

This chapter provides information on configuring remote management.

11.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyXEL Device interface (if any) from which computers.

You may manage your ZyXEL Device from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only,
- Neither (Disable).

To disable remote management of a service, select **Disable** in the corresponding **Access Status** field.

You may only have one remote management session running at a time. The ZyXEL Device automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. Telnet
2. HTTP

11.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- You have disabled that service in one of the remote management screens.
- The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
- There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

11.1.2 Remote Management and NAT

When NAT is enabled:

- Use the ZyXEL Device's WAN IP address when configuring from the WAN.
- Use the ZyXEL Device's LAN IP address when configuring from the LAN.

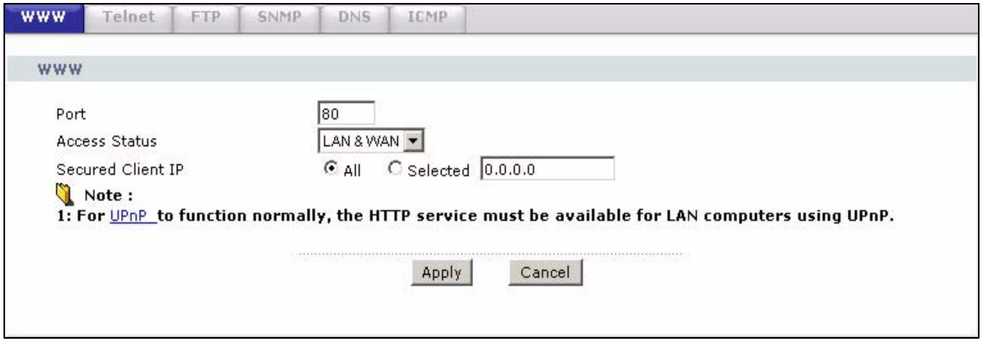
11.1.3 System Timeout

There is a system management idle timeout. The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. The default value is five minutes, and you can change or disable this in Section 13.1.2 on page 143.

11.2 WWW

Use this screen to change your ZyXEL Device's World Wide Web settings. Click **Advanced > Remote MGMT** to display the **WWW** screen.

Figure 53 Remote MGMT > WWW



Port: 80
Access Status: LAN & WAN
Secured Client IP: ● All ○ Selected 0.0.0.0

Note :
1: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

The following table describes the labels in this screen.

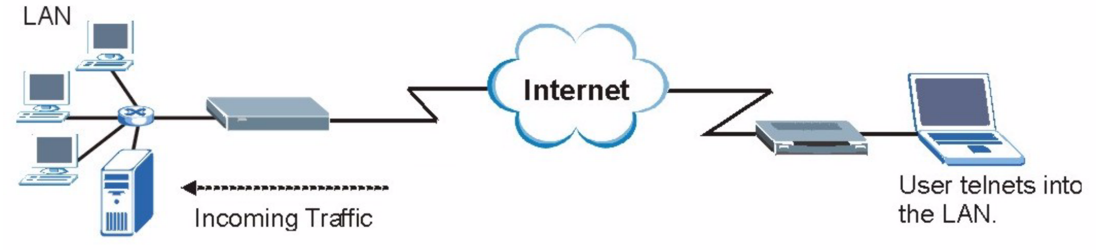
Table 34 Remote MGMT > WWW

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your settings back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.3 Telnet

You can configure your ZyXEL Device for remote Telnet access as shown next. The administrator uses Telnet from a computer on a remote network to access the ZyXEL Device.

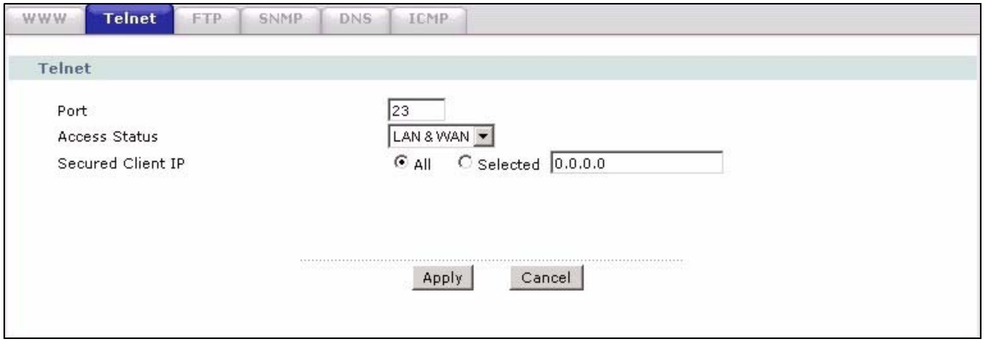
Figure 54 Telnet Configuration on a TCP/IP Network



11.4 Configuring Telnet

See Section 11.1 on page 119 for background information. Use this screen to configure Telnet access to the ZyXEL Device. Click **Advanced > Remote MGMT** > **Telnet** tab to display the screen as shown.

Figure 55 Remote MGMT > Telnet



Telnet

Port 23

Access Status LAN & WAN

Secured Client IP ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

Table 35 Remote MGMT > Telnet

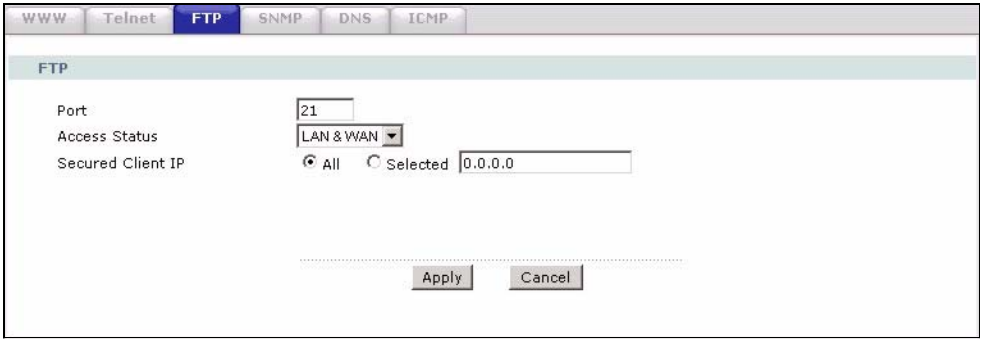
LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.5 Configuring FTP

You can upload and download the ZyXEL Device's firmware and configuration files using FTP, please see the chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

See Section 11.1 on page 119 for background information. Use this screen to control FTP access to the ZyXEL Device. To change your ZyXEL Device's FTP settings, click **Advanced** > **Remote MGMT** > **FTP** tab. The screen appears as shown.

Figure 56 Remote MGMT > FTP



Port: 21

Access Status: LAN & WAN

Secured Client IP: ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

Table 36 Remote MGMT > FTP

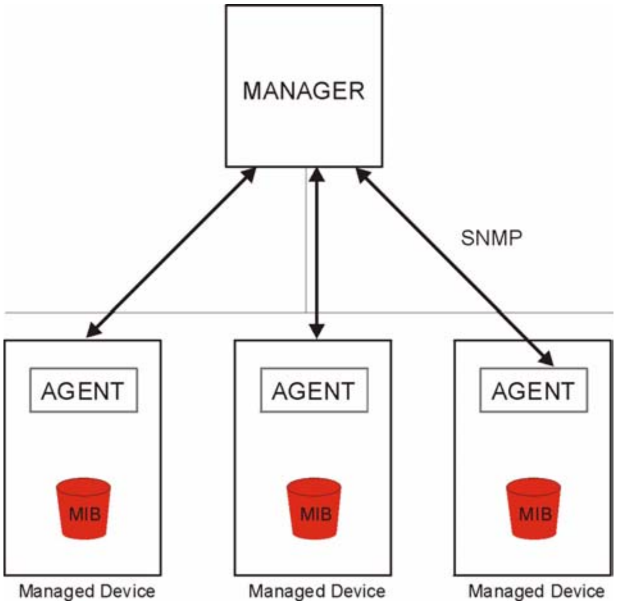
LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.6 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

SNMP is only available if TCP/IP is configured.

Figure 57 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyXEL Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

11.6.1 Supported MIBs

The ZyXEL Device supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

11.6.2 SNMP Traps

The ZyXEL Device will send traps to the SNMP manager when any one of the following events occurs:

Table 37 SNMPv1 Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

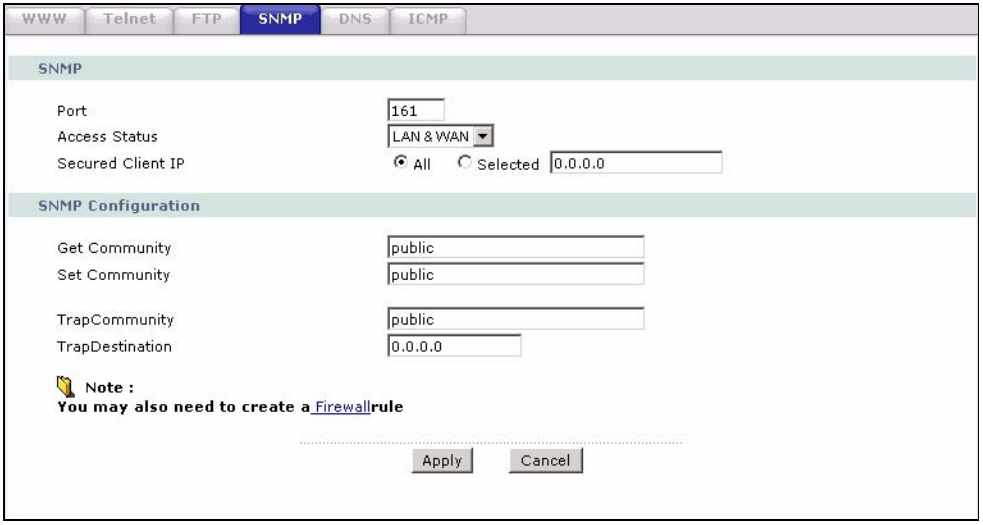
Table 38 SNMPv2 Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
SNMPv2 Traps		
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the switch is turned on.
WarmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the switch restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.

11.6.3 Configuring SNMP

See Section 11.1 on page 119 for background information. Use this screen to change your ZyXEL Device’s SNMP settings. Click **Advanced > Remote MGMT** > **SNMP**. The screen appears as shown.

Figure 58 Remote MGMT > SNMP



SNMP

Port: 161

Access Status: LAN & WAN

Secured Client IP: ● All ○ Selected 0.0.0.0

SNMP Configuration

Get Community: public

Set Community: public

TrapCommunity: public

TrapDestination: 0.0.0.0

Note :
You may also need to create a Firewall**rule**

The following table describes the labels in this screen.

Table 39 Remote MGMT > SNMP

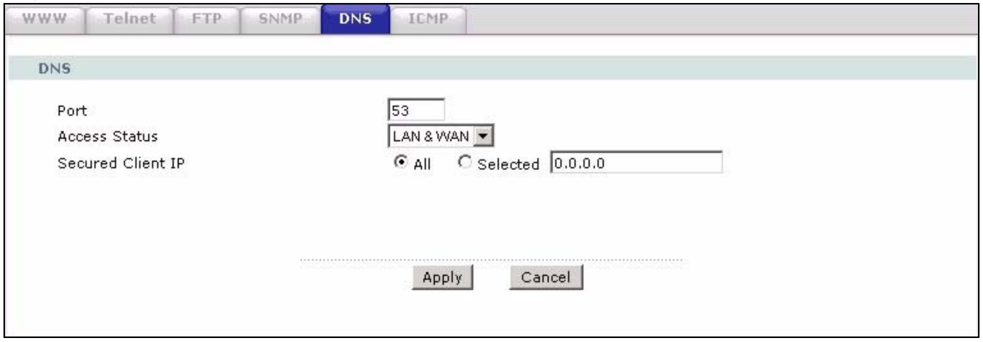
LABEL	DESCRIPTION
SNMP	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a “trusted” computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.7 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to the chapter on LAN for background information.

See Section 11.1 on page 119 for background information. Click **Advanced** > **Remote MGMT** > **DNS**. The screen appears as shown. Use this screen to set from which IP address the ZyXEL Device will accept DNS queries and on which interface it can send them your ZyXEL Device's DNS settings.

Figure 59 Remote MGMT > DNS



DNS

Port: 53

Access Status: LAN & WAN

Secured Client IP: ● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

Table 40 Remote MGMT > DNS

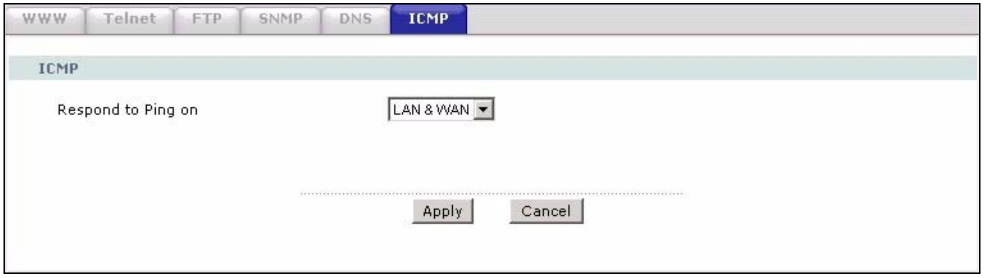
LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may send DNS queries to the ZyXEL Device.
Secured Client IP	A secured client is a "trusted" computer that is allowed to send DNS queries to the ZyXEL Device. Select **All** to allow any computer to send DNS queries to the ZyXEL Device. Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the ZyXEL Device.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.8 Configuring ICMP

Use this screen to control how the ZyXEL Device responds to other types of requests. Click **Advanced > Remote MGMT** > **ICMP**. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. Your ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.

Figure 60 Remote MGMT > ICMP



ICMP

Respond to Ping on: LAN & WAN

The following table describes the labels in this screen.

Table 41 Remote MGMT > ICMP

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The ZyXEL Device will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise, select **LAN & WAN** to reply to both incoming LAN and WAN Ping requests.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to begin configuring this screen afresh.

12

Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

12.1 Introducing Universal Plug and Play

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

See Section 12.2.1 on page 130 for configuration instructions.

12.1.1 How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

12.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

12.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the ZyXEL Device allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

12.2 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

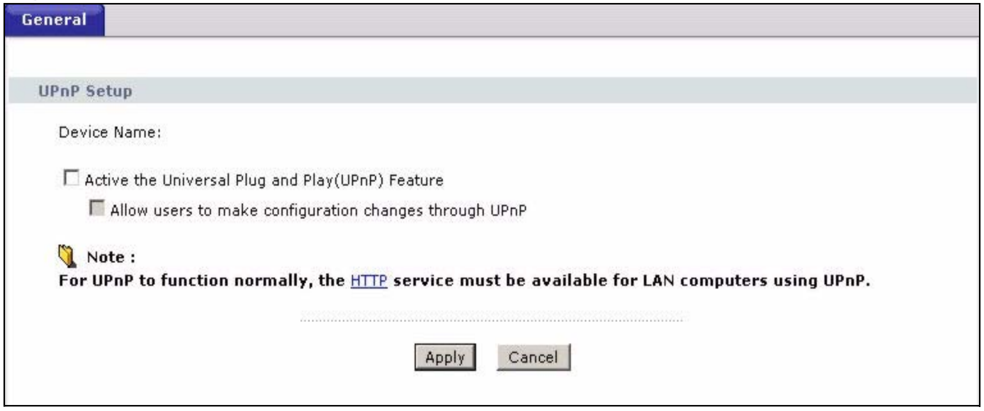
See the following sections for examples of installing and using UPnP.

12.2.1 Configuring UPnP

Use this screen to set up UPnP in the ZyXEL Device. Click **Advanced > UPnP** to display the screen shown next.

See Section 12.1 on page 129 for more information.

Figure 61 UPnP > General



General
UPnP Setup
Device Name:
□ Active the Universal Plug and Play(UPnP) Feature
□ Allow users to make configuration changes through UPnP
Note :
For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.
Apply
Cancel

The following table describes the fields in this screen.

Table 42 UPnP > General

LABEL	DESCRIPTION
Active the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyXEL Device so that they can communicate through the ZyXEL Device, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Apply	Click **Apply** to save the setting to the ZyXEL Device.
Cancel	Click **Cancel** to return to the previously saved settings.

12.3 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

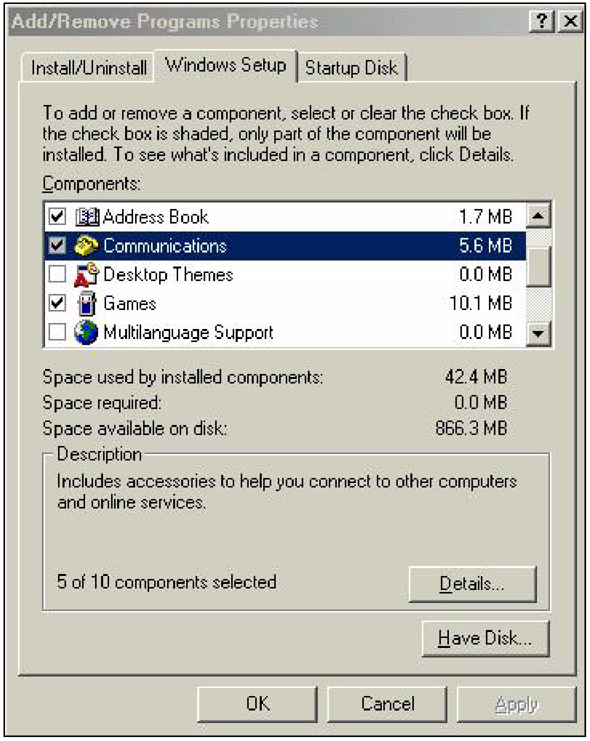
Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 62 Add/Remove Programs: Windows Setup: Communication



Add/Remove Programs Properties

Install/Uninstall | Windows Setup | Startup Disk

To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Address Book	1.7 MB
☑	Communications	5.6 MB
□	Desktop Themes	0.0 MB
☑	Games	10.1 MB
□	Multilanguage Support	0.0 MB

Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

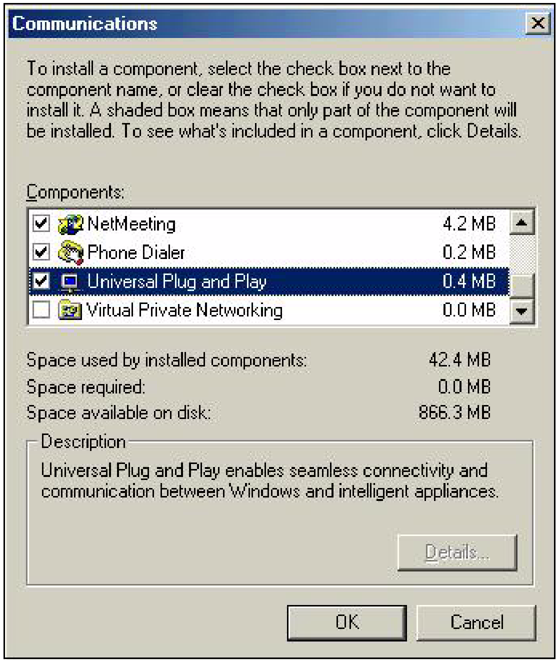
Description

Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 63 Add/Remove Programs: Windows Setup: Communication: Components



Communications

To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	NetMeeting	4.2 MB
☑	Phone Dialer	0.2 MB
☑	Universal Plug and Play	0.4 MB
☐	Virtual Private Networking	0.0 MB

Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

Description

Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

Installing UPnP in Windows XP

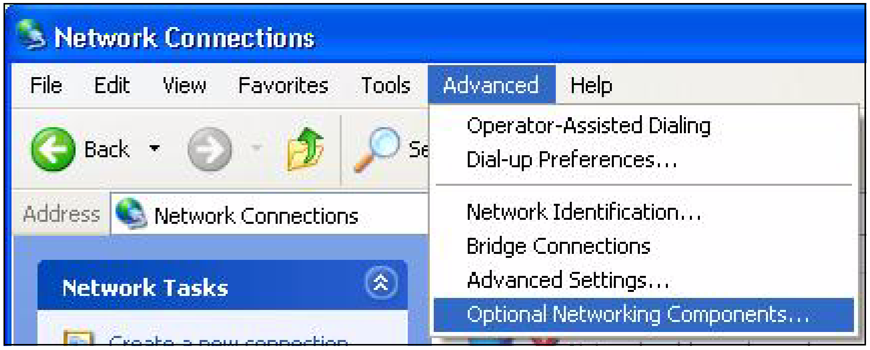
Follow the steps below to install the UPnP in Windows XP.

1 Click **Start** and **Control Panel**.

2 Double-click **Network Connections**.

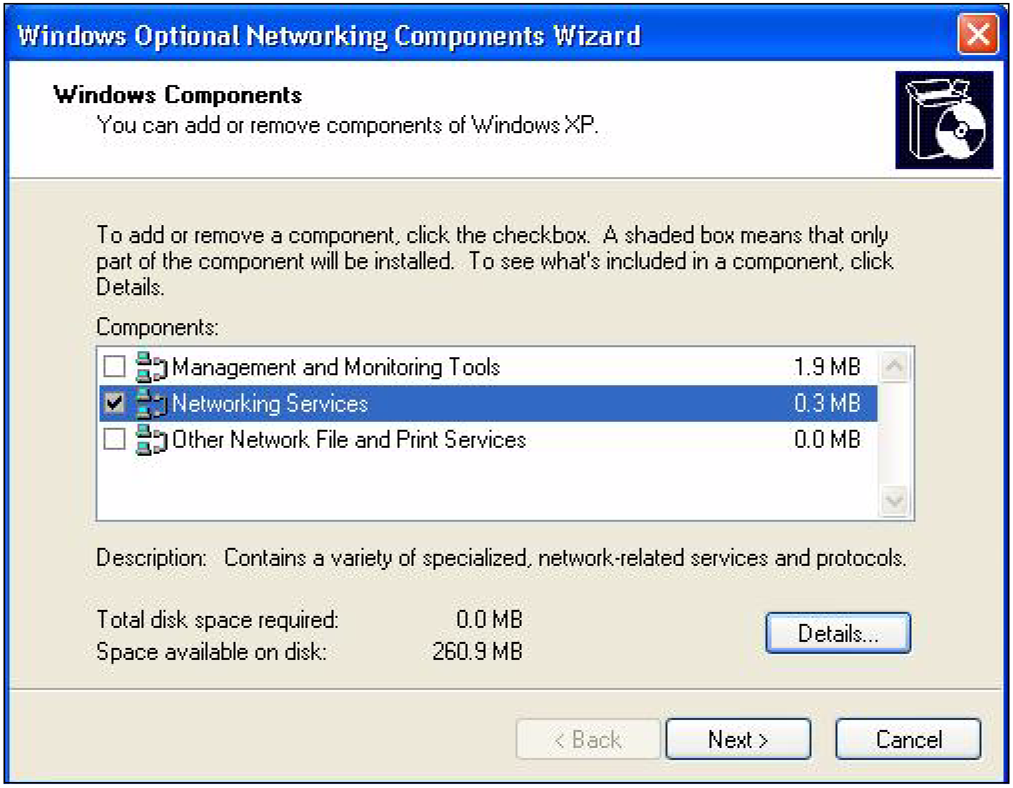
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**

Figure 64 Network Connections



4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 65 Windows Optional Networking Components Wizard



Windows Optional Networking Components Wizard

Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

□	Management and Monitoring Tools	1.9 MB
☑	Networking Services	0.3 MB
□	Other Network File and Print Services	0.0 MB

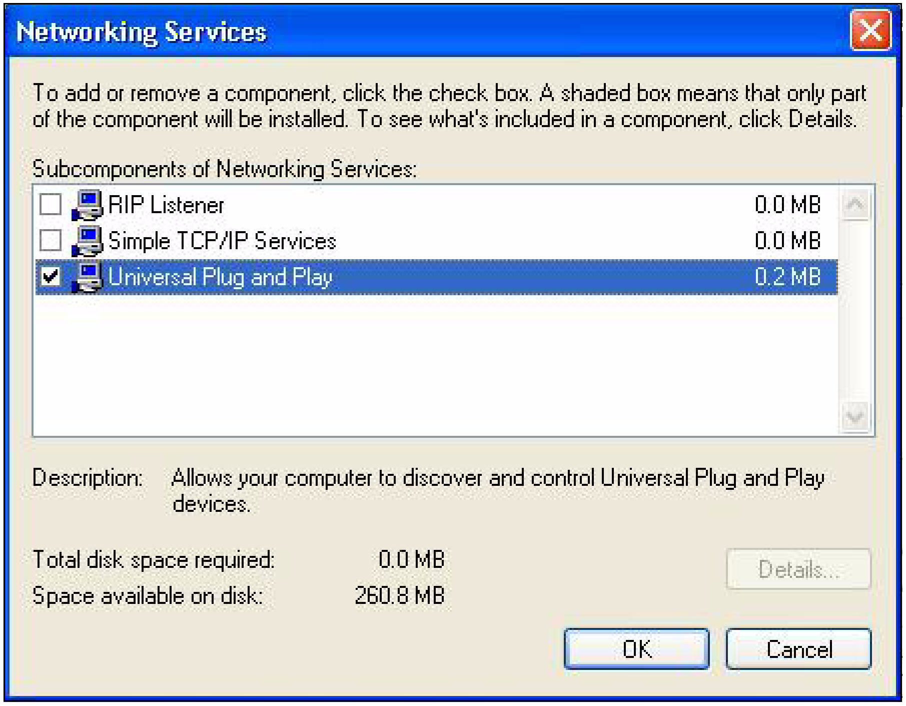
Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 260.9 MB

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 66 Networking Services



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

□	RIP Listener	0.0 MB
□	Simple TCP/IP Services	0.0 MB
☑	Universal Plug and Play	0.2 MB

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 0.0 MB

Space available on disk: 260.8 MB

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

12.4 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL Device.

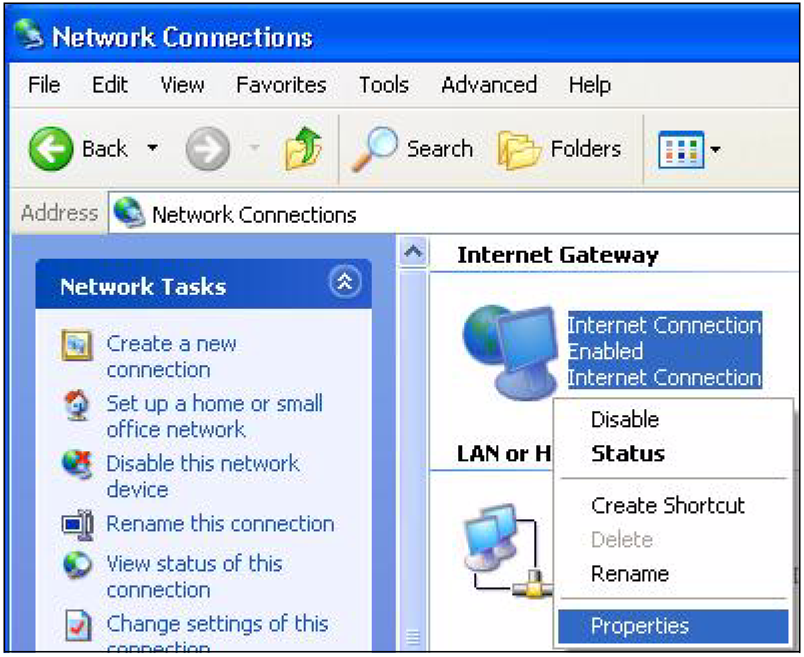
Make sure the computer is connected to a LAN port of the ZyXEL Device. Turn on your computer and the ZyXEL Device.

Auto-discover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

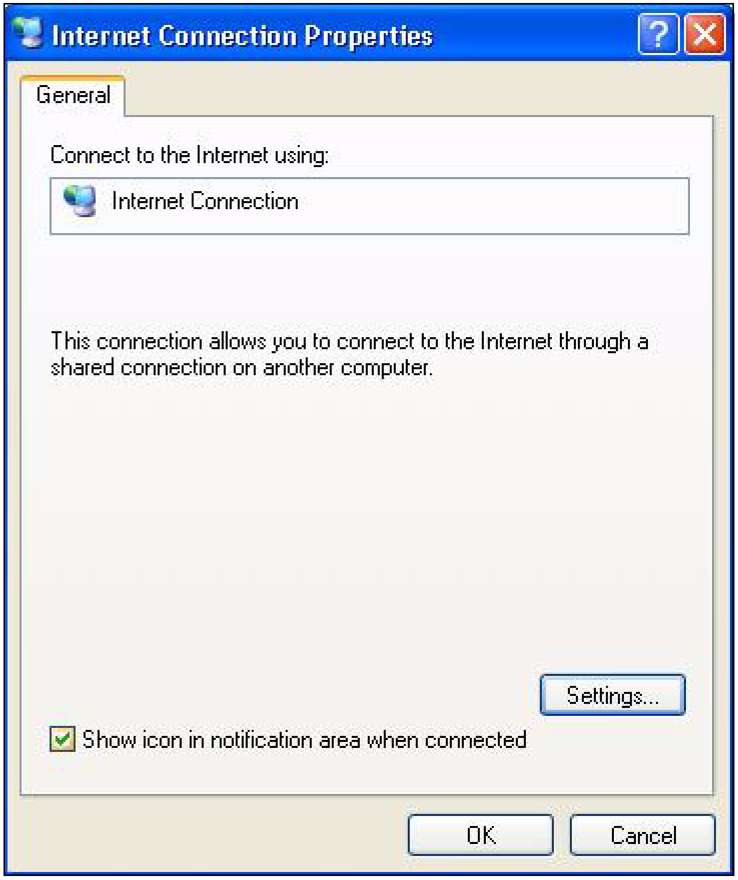
2 Right-click the icon and select **Properties**.

Figure 67 Network Connections



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 68 Internet Connection Properties



Connect to the Internet using:

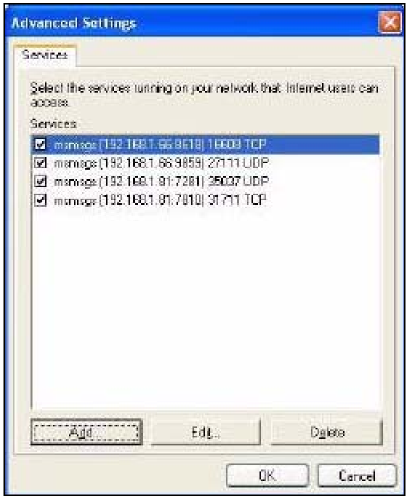
Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 69 Internet Connection Properties: Advanced Settings

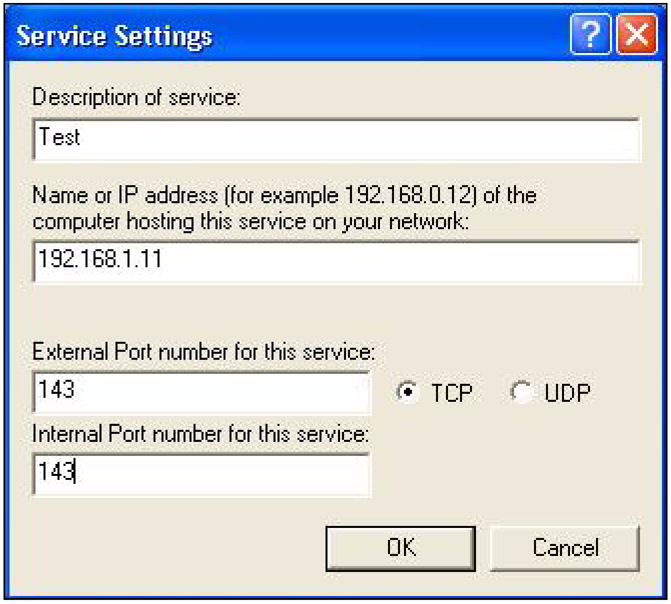


Select the services running on your network that Internet users can access.

Services

☑ msmsgs (192.168.1.66:8618) 16608 TCP
☑ msmsgs (192.168.1.66:9859) 27111 UDP
☑ msmsgs (192.168.1.81:7281) 35037 UDP
☑ msmsgs (192.168.1.81:7810) 31711 TCP

Figure 70 Internet Connection Properties: Advanced Settings: Add



Description of service: Test

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network: 192.168.1.11

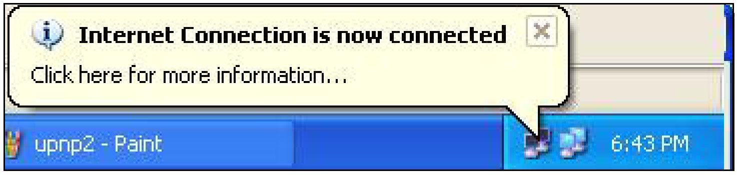
External Port number for this service: 143 ● TCP ○ UDP

Internal Port number for this service: 143

5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

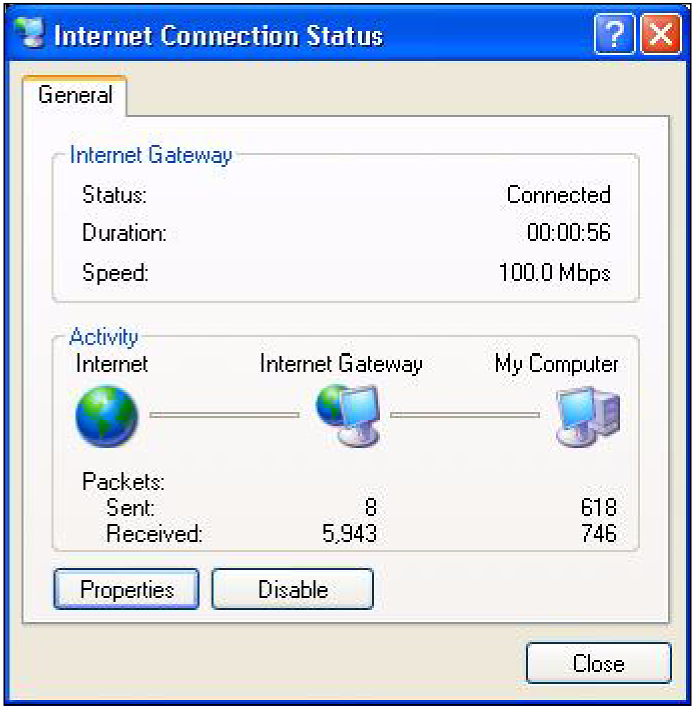
Figure 71 System Tray Icon


Internet Connection is now connected

Click here for more information...

7 Double-click on the icon to display your current Internet connection status.

Figure 72 Internet Connection Status



Status: Connected
Duration: 00:00:56
Speed: 100.0 Mbps

Packets:
Sent: 8 618
Received: 5,943 746

Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This comes helpful if you do not know the IP address of the ZyXEL Device.

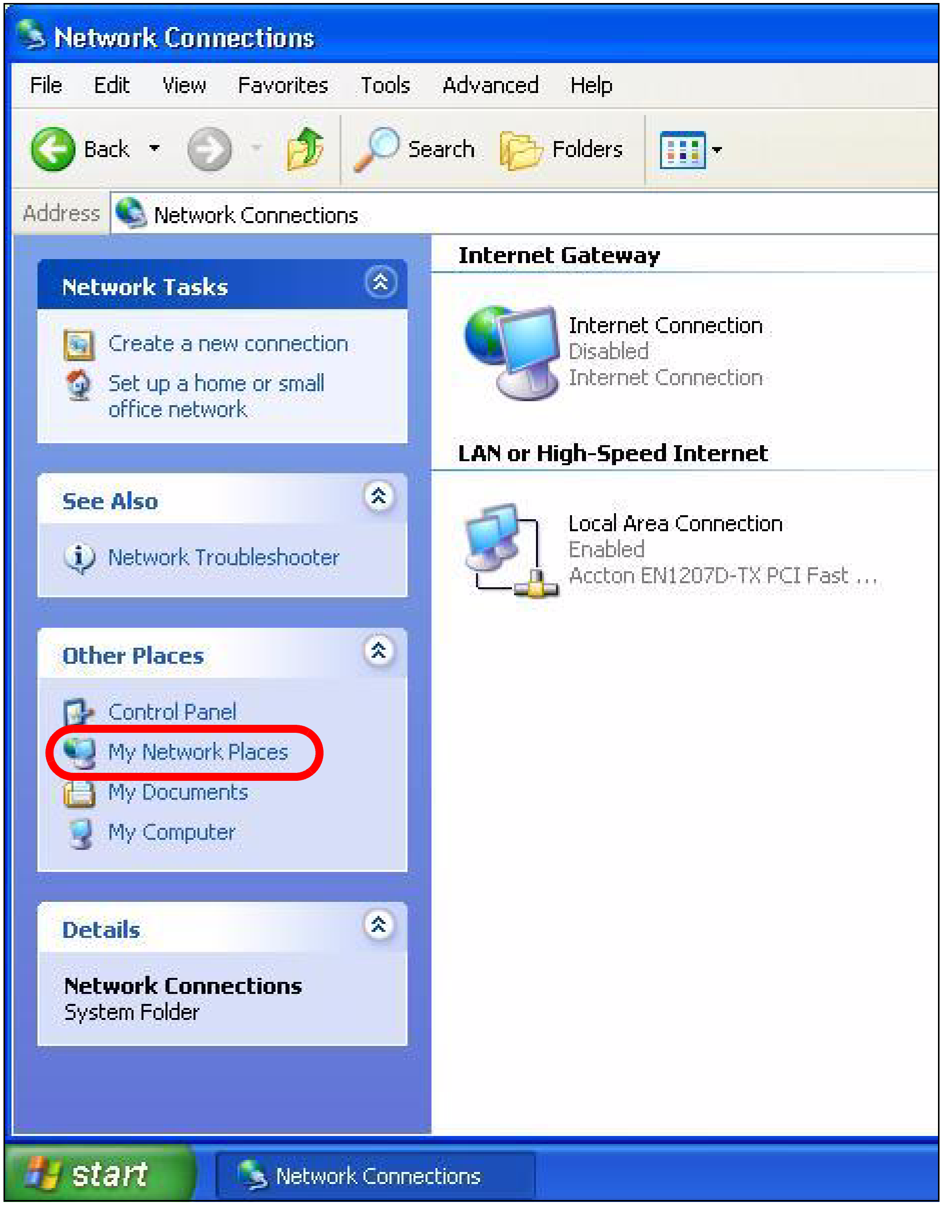
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

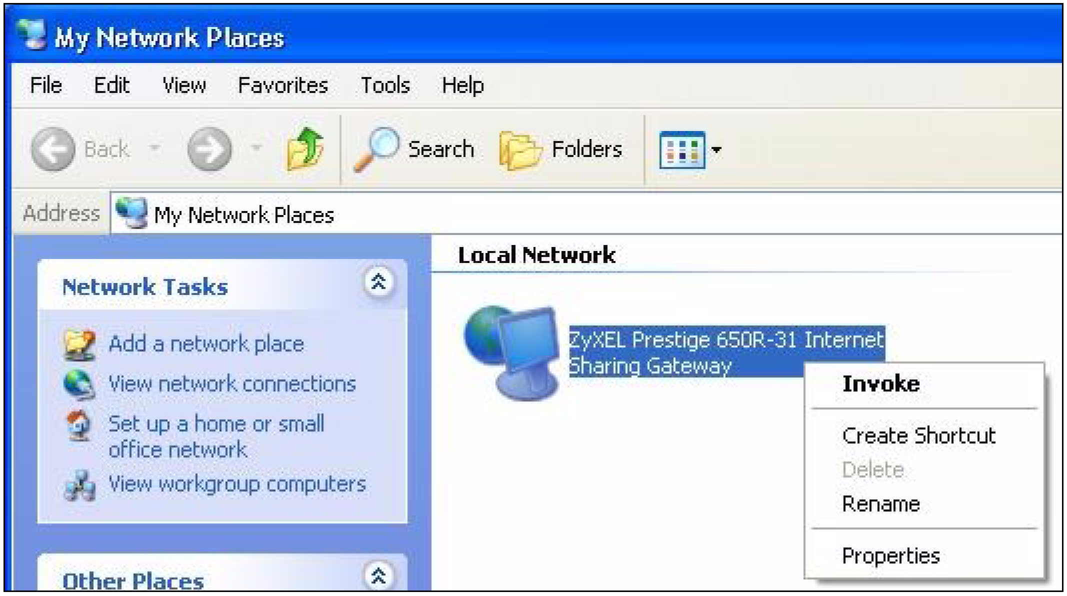
Figure 73 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

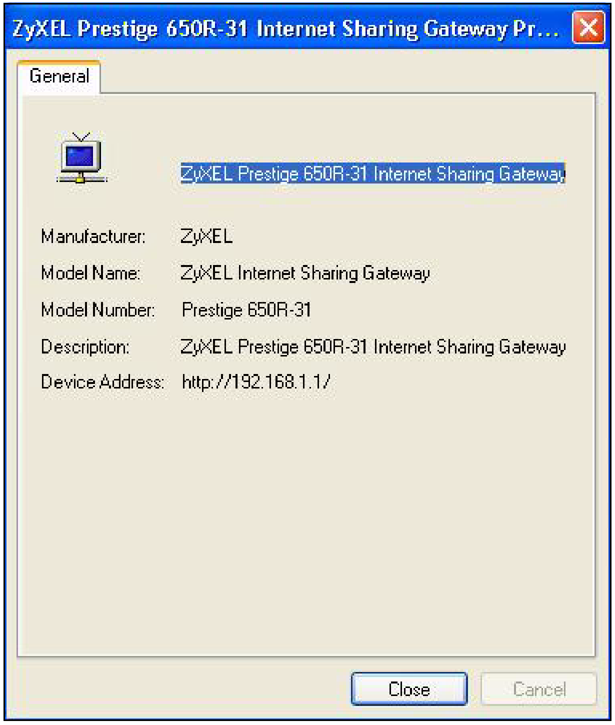
5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.

Figure 74   Network Connections: My Network Places



6 Right-click on the icon for your ZyXEL Device and select **Properties**. A properties window displays with basic information about the ZyXEL Device.

Figure 75   Network Connections: My Network Places: Properties: Example



ZyXEL Prestige 650R-31 Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number: Prestige 650R-31

Description: ZyXEL Prestige 650R-31 Internet Sharing Gateway

Device Address: http://192.168.1.1/

PART V
Maintenance

13

System

This chapter explains how to configure the ZyXEL Device's system name, domain name, password, and time and date settings.

13.1 General Setup

13.1.1 General Setup and System Name

General Setup contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

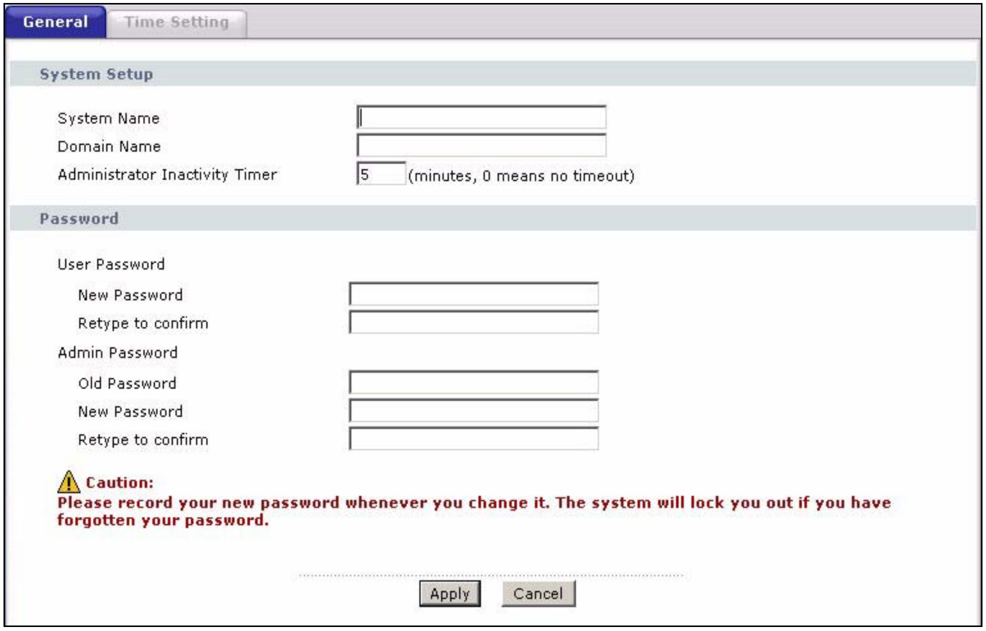
- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyXEL Device **System Name**.

13.1.2 General Setup

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name), the domain name can be assigned from the ZyXEL Device via DHCP.

Use this screen to set up the ZyXEL Device's system name, domain name, inactivity timer, and passwords. Click **Maintenance > System** to open the **General** screen.

Figure 76 System > General


General
Time Setting
System Setup
System Name
Domain Name
Administrator Inactivity Timer
5
(minutes, 0 means no timeout)
Password
User Password
New Password
Retype to confirm
Admin Password
Old Password
New Password
Retype to confirm
Caution:
Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.
Apply
Cancel

The following table describes the labels in this screen.

Table 43 System > General

LABEL	DESCRIPTION
System Setup	
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or CLI (Command Line Interpreter)) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Password	
User Password	If you log in with the user password, you can only view the ZyXEL Device status. The default user password is **user**.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Retype to Confirm	Type the new password again for confirmation.
Admin Password	In addition to the wizard setup, a user logs in with the admin password can also view and configure the advanced features on the ZyXEL Device.
Old Password	Type the default administrator password (**1234**) or the existing password you use to access the system for configuring advanced features in this field.

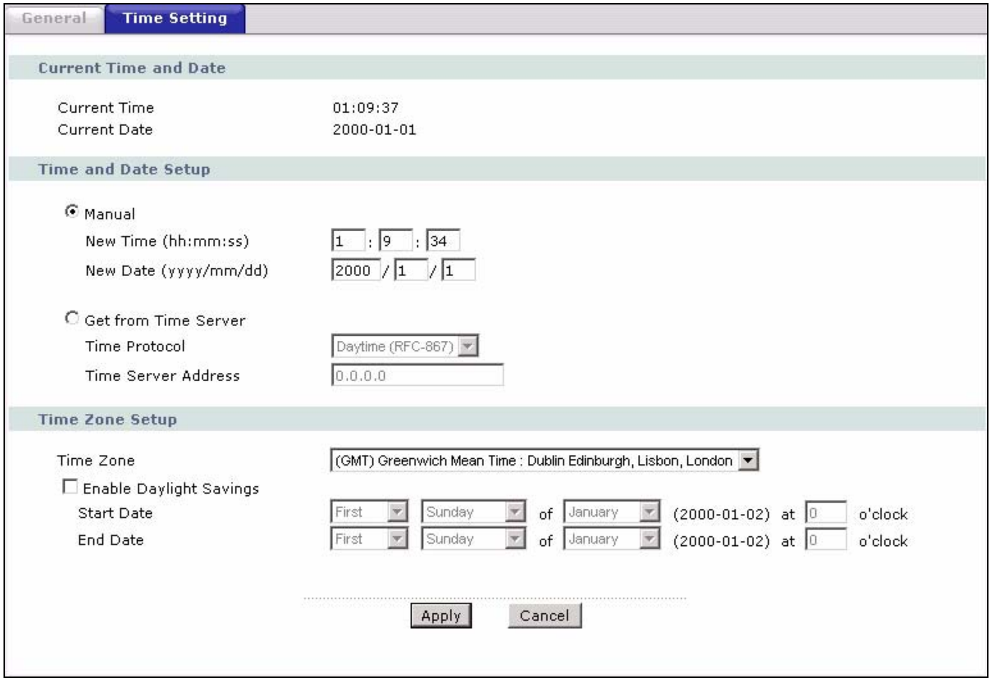
Table 43 System > General (continued)

LABEL	DESCRIPTION
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.2 Time Setting

To change your ZyXEL Device's time and date, click **Maintenance** > **System** > **Time Setting**. The screen appears as shown. Use this screen to configure the ZyXEL Device's time based on your local time zone.

Figure 77 System > Time Setting



Current Time and Date

Current Time	01:09:37
Current Date	2000-01-01

Time and Date Setup

● Manual

New Time (hh:mm:ss)	1 : 9 : 34
New Date (yyyy/mm/dd)	2000 / 1 / 1

○ Get from Time Server

Time Protocol	Daytime (RFC-867)
Time Server Address	0.0.0.0

Time Zone Setup

Time Zone	(GMT) Greenwich Mean Time : Dublin Edinburgh, Lisbon, London

□ Enable Daylight Savings

Start Date	First Sunday of January (2000-01-02) at 0 o'clock
End Date	First Sunday of January (2000-01-02) at 0 o'clock

The following table describes the fields in this screen.

Table 44 System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the time with the time server.
Current Date	This field displays the date of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the date with the time server.

Table 44 System > Time Setting

LABEL	DESCRIPTION
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the ZyXEL Device get the time and date from the time server you specified below.
Time Protocol	Select the time service protocol that your time server sends when you turn on the ZyXEL Device. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC 1305)**, is similar to Time (RFC 868).
Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and **2:00**. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 44 System > Time Setting

LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and **2:00**. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14

Logs

This chapter contains information about configuring general log settings and viewing the ZyXEL Device's logs. Refer to the appendix for example log message explanations.

14.1 Logs Overview

The web configurator allows you to choose which categories of events and/or alerts to have the ZyXEL Device log and then display the logs or have the ZyXEL Device send them to an administrator (as e-mail) or to a syslog server.

14.1.1 Alerts and Logs

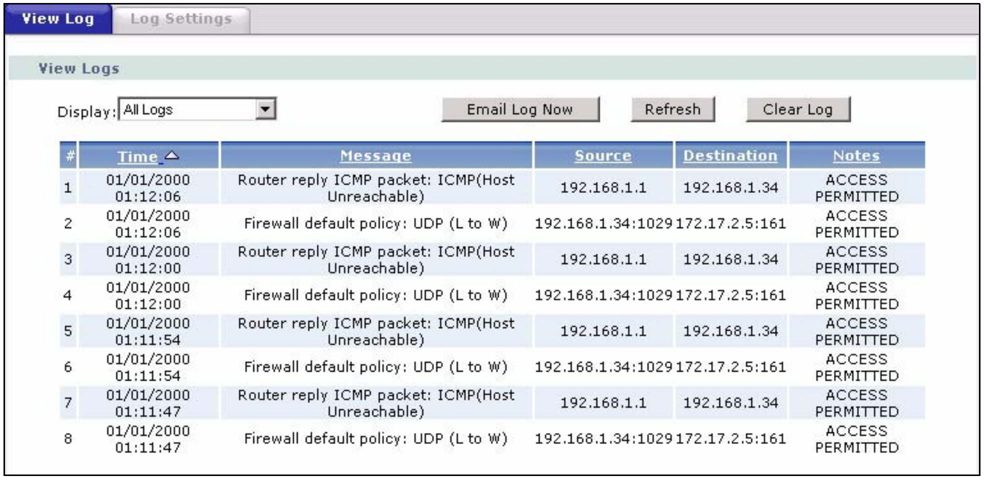
An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

14.2 Viewing the Logs

Click **Maintenance > Logs** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 14.3 on page 150).

Log entries in red indicate alerts. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 78 Logs > View Log



Display: All Logs

#	Time	Message	Source	Destination	Notes
1	01/01/2000 01:12:06	Router reply ICMP packet: ICMP(Host Unreachable)	192.168.1.1	192.168.1.34	ACCESS PERMITTED
2	01/01/2000 01:12:06	Firewall default policy: UDP (L to W)	192.168.1.34:1029	172.17.2.5:161	ACCESS PERMITTED
3	01/01/2000 01:12:00	Router reply ICMP packet: ICMP(Host Unreachable)	192.168.1.1	192.168.1.34	ACCESS PERMITTED
4	01/01/2000 01:12:00	Firewall default policy: UDP (L to W)	192.168.1.34:1029	172.17.2.5:161	ACCESS PERMITTED
5	01/01/2000 01:11:54	Router reply ICMP packet: ICMP(Host Unreachable)	192.168.1.1	192.168.1.34	ACCESS PERMITTED
6	01/01/2000 01:11:54	Firewall default policy: UDP (L to W)	192.168.1.34:1029	172.17.2.5:161	ACCESS PERMITTED
7	01/01/2000 01:11:47	Router reply ICMP packet: ICMP(Host Unreachable)	192.168.1.1	192.168.1.34	ACCESS PERMITTED
8	01/01/2000 01:11:47	Firewall default policy: UDP (L to W)	192.168.1.34:1029	172.17.2.5:161	ACCESS PERMITTED

The following table describes the fields in this screen.

Table 45 Logs > View Log

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** screen display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **E-mail Log Settings** fields in **Log Settings**).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.
#	This field displays an index number.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.

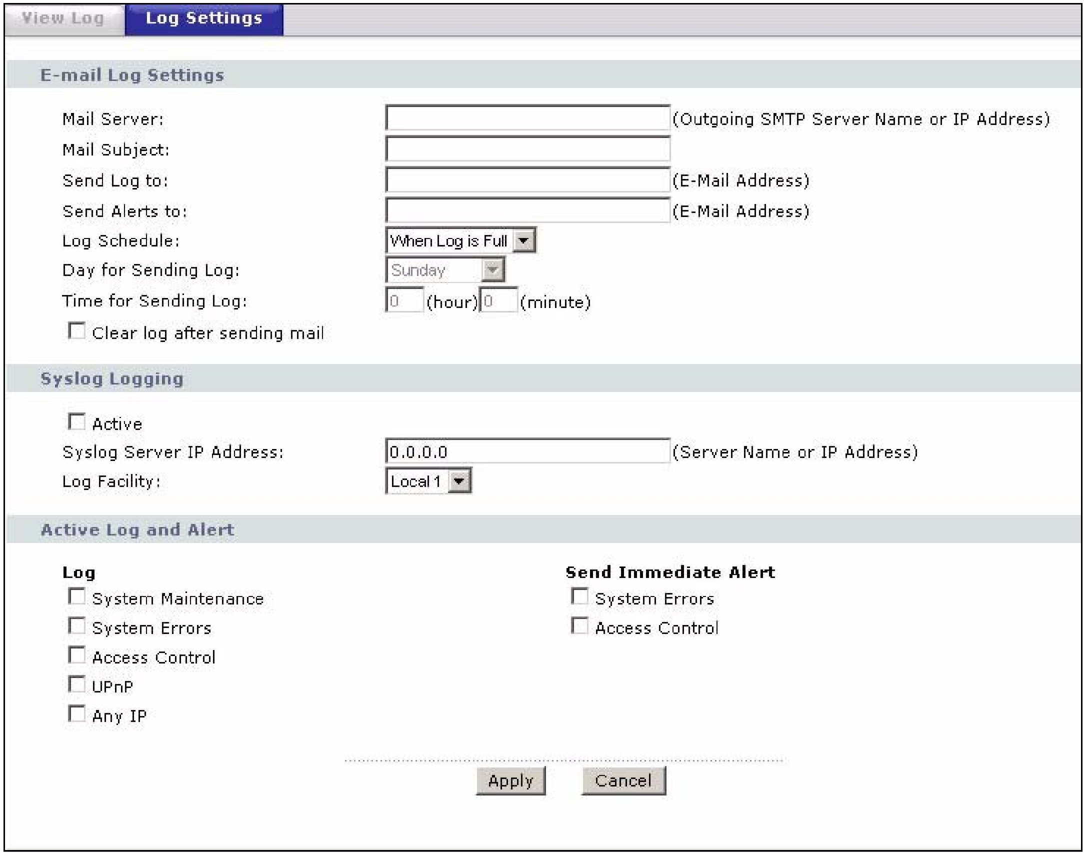
14.3 Configuring Log Settings

See Section 14.1 on page 149 for background information. Use the **Log Settings** screen to configure where the ZyXEL Device is to send logs; the schedule for when the ZyXEL Device is to send the logs and which logs and/or immediate alerts the ZyXEL Device is to record. See Section 14.1 on page 149 for more information.

To change your ZyXEL Device's log settings, click **Maintenance > Logs** > **Log Settings**. The screen appears as shown.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full. Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

Figure 79 Logs > Log Settings



E-mail Log Settings

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Subject:

Send Log to: (E-Mail Address)

Send Alerts to: (E-Mail Address)

Log Schedule: When Log is Full

Day for Sending Log: Sunday

Time for Sending Log: 0 (hour) 0 (minute)

□ Clear log after sending mail

Syslog Logging

□ Active

Syslog Server IP Address: 0.0.0.0 (Server Name or IP Address)

Log Facility: Local 1

Active Log and Alert

Log

□ System Maintenance

□ System Errors

□ Access Control

□ UPnP

□ Any IP

Send Immediate Alert

□ System Errors

□ Access Control

The following table describes the fields in this screen.

Table 46 Logs > Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL Device sends. Not all ZyXEL Device models have this field.
Send Log To	The ZyXEL Device sends logs to the e-mail address specified in this field. If this field is left blank, the ZyXEL Device does not send logs via e-mail.
Send Alerts To	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.

Table 46 Logs > Log Settings

LABEL	DESCRIPTION
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: **Daily** **Weekly** **Hourly** **When Log is Full** **None.** If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the check box to delete all the logs after the ZyXEL Device sends an E-mail of the logs.
Syslog Logging	The ZyXEL Device sends a log to an external syslog server.
Active	Click **Active** to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the ZyXEL Device to send E-mail alerts immediately.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return to the previously saved settings.

15

Tools

This chapter covers uploading new firmware, managing configuration and restarting your ZyXEL Device.

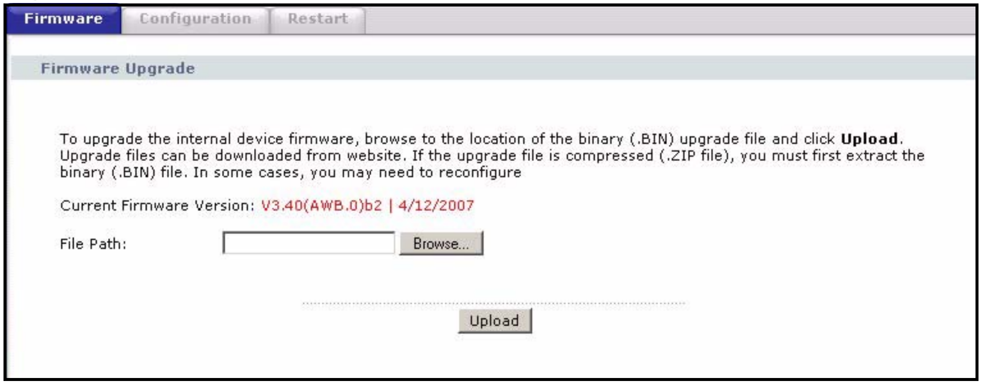
15.1 Firmware Upgrade

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, “ZyXEL Device.bin”. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Only use firmware for your device’s specific model. Refer to the label on the bottom of your device.

Click **Maintenance** > **Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device.

Figure 80 Tools > Firmware



To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click **Upload**. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure

Current Firmware Version: V3.40(AWB.0)b2 | 4/12/2007

File Path:

The following table describes the labels in this screen.

Table 47 Tools > Firmware

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.

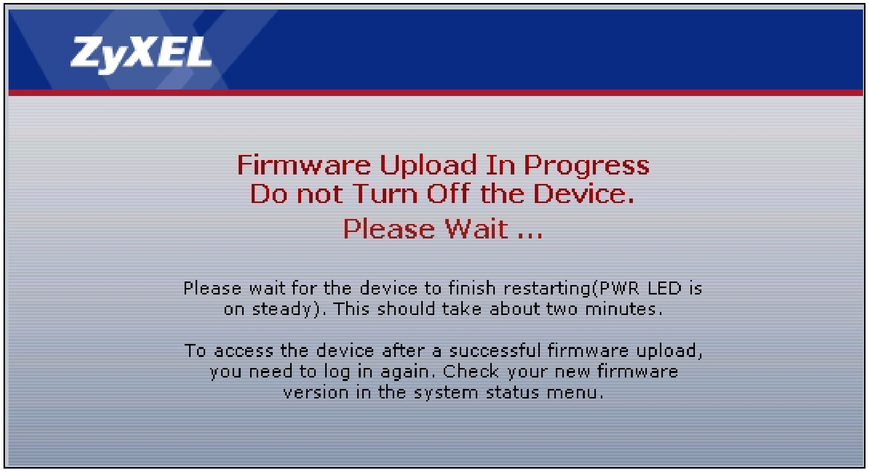
Table 47 Tools > Firmware (continued)

LABEL	DESCRIPTION
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes. Note: Do not turn off the device while firmware upload is in progress.

Do NOT turn off the ZyXEL Device while firmware upload is in progress!

After you see the **Firmware Upload in Progress** screen, wait two minutes before logging into the ZyXEL Device again.

Figure 81 Firmware Upload In Progress



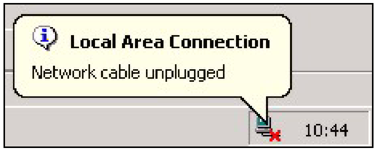
Firmware Upload In Progress
Do not Turn Off the Device.
Please Wait ...

Please wait for the device to finish restarting(PWR LED is on steady). This should take about two minutes.

To access the device after a successful firmware upload, you need to log in again. Check your new firmware version in the system status menu.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

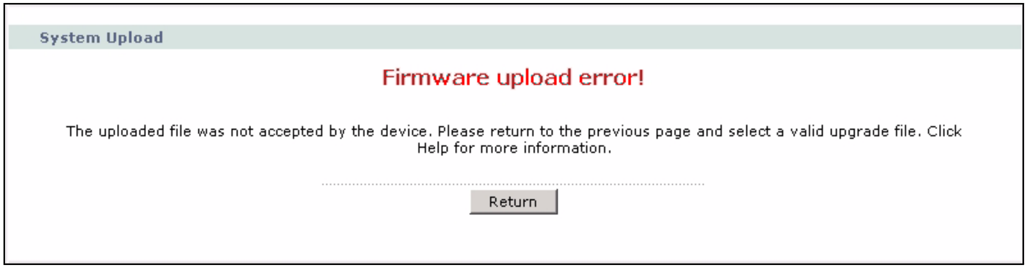
Figure 82 Network Temporarily Disconnected


Local Area Connection
Network cable unplugged

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

Figure 83 Error Message



System Upload

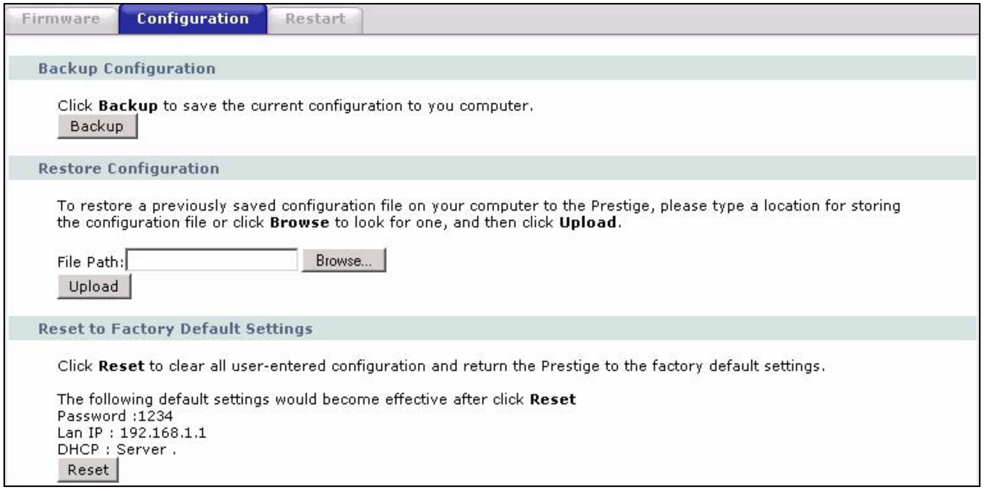
Firmware upload error!

The uploaded file was not accepted by the device. Please return to the previous page and select a valid upgrade file. Click Help for more information.

15.2 Configuration

Use this screen to back up or restore the configuration of the ZyXEL Device. You can also use this screen to reset the ZyXEL Device to the factory default settings. To access this screen, click **Maintenance** > **Tools** > **Configuration**.

Figure 84 Tools > Configuration



Backup Configuration

Click **Backup** to save the current configuration to you computer.

Restore Configuration

To restore a previously saved configuration file on your computer to the Prestige, please type a location for storing the configuration file or click **Browse** to look for one, and then click **Upload**.

File Path:

Reset to Factory Default Settings

Click **Reset** to clear all user-entered configuration and return the Prestige to the factory default settings.

The following default settings would become effective after click **Reset**
Password :1234
Lan IP : 192.168.1.1
DHCP : Server .

The following table describes the labels in this screen.

Table 48 Tools > Configuration

LABEL	DESCRIPTION
Backup Configuration	
Backup	Click this to save the ZyXEL Device's current configuration to a file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file is useful if you need to return to your previous settings.
Restore Configuration	
File Path	Enter the location of the file you want to upload, or click **Browse...** to find it.
Browse	Click this to find the file you want to upload.

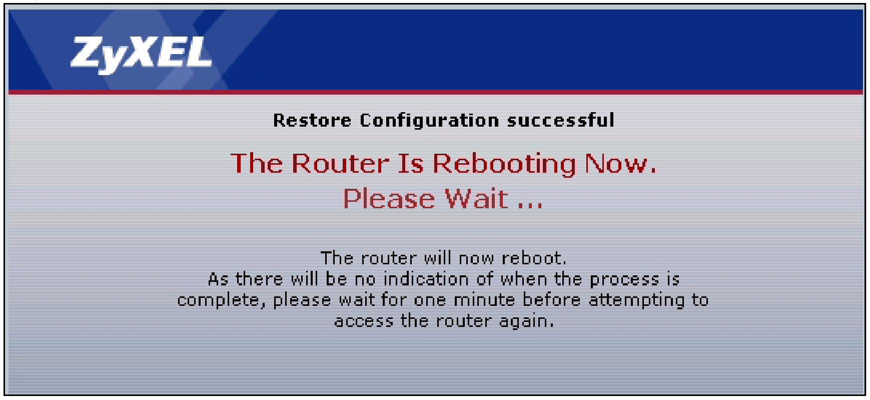
Table 48 Tools > Configuration (continued)

LABEL	DESCRIPTION
Upload	Click this to restore the selected configuration file. See below for more information about this. Note: Do not turn off the device while configuration file upload is in progress.
Reset to Factory Default Settings	
Reset	Click this to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults. There is no warning screen. See Section 2.5 on page 45 for more information about resetting the ZyXEL Device.

Do not turn off the device while configuration file upload is in progress.

When the ZyXEL Device has finished restoring the selected configuration file, the following screen appears.

Figure 85 Configuration Upload Successful



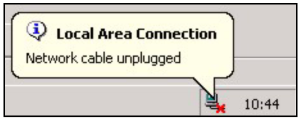
Restore Configuration successful

The Router Is Rebooting Now.
Please Wait ...

The router will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

The device now automatically restarts. This causes a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 86 Network Temporarily Disconnected



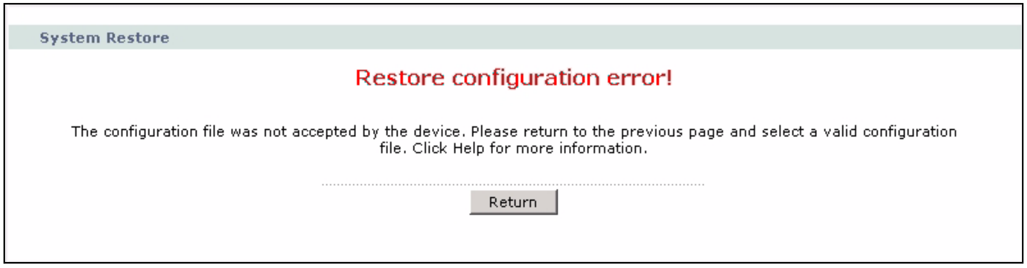
Local Area Connection
Network cable unplugged

If the ZyXEL Device's IP address is different in the configuration file you selected, you may need to change the IP address of your computer to be in the same subnet as that of the ZyXEL Device. See your Quick Start Guide or the appendices for details on how to set up your computer's IP address.

You might have to open a new browser to log in again.

If the upload was not successful, a **Configuration Upload Error** screen appears.

Figure 87 Configuration Upload Error



System Restore

Restore configuration error!

The configuration file was not accepted by the device. Please return to the previous page and select a valid configuration file. Click Help for more information.

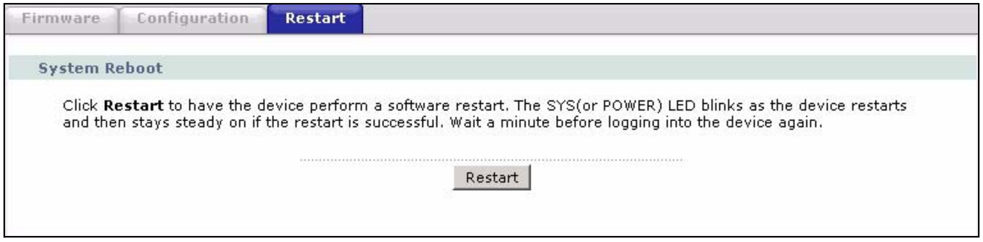
Click **Return** to go back to the previous screen.

15.3 Restart

System restart allows you to reboot the ZyXEL Device without turning the power off.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

Figure 88 Tools > Restart



System Reboot

Click **Restart** to have the device perform a software restart. The SYS(or POWER) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.

16

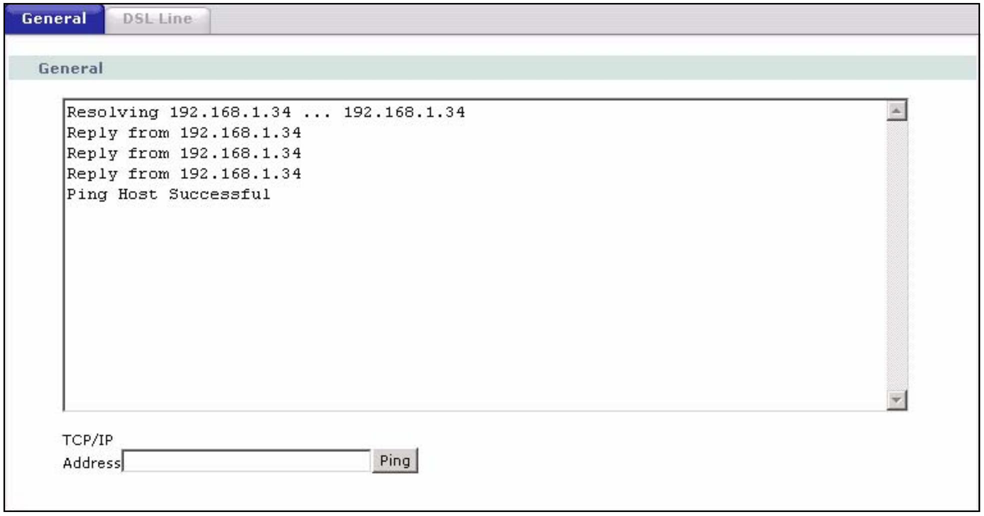
Diagnostic

These read-only screens display information to help you identify problems with the ZyXEL Device.

16.1 General Diagnostic

Use this screen to ping a computer on the network. Click **Maintenance > Diagnostic** to open the screen shown next.

Figure 89 Diagnostic > General



```
Resolving 192.168.1.34 ... 192.168.1.34
Reply from 192.168.1.34
Reply from 192.168.1.34
Reply from 192.168.1.34
Ping Host Successful
```

The following table describes the fields in this screen.

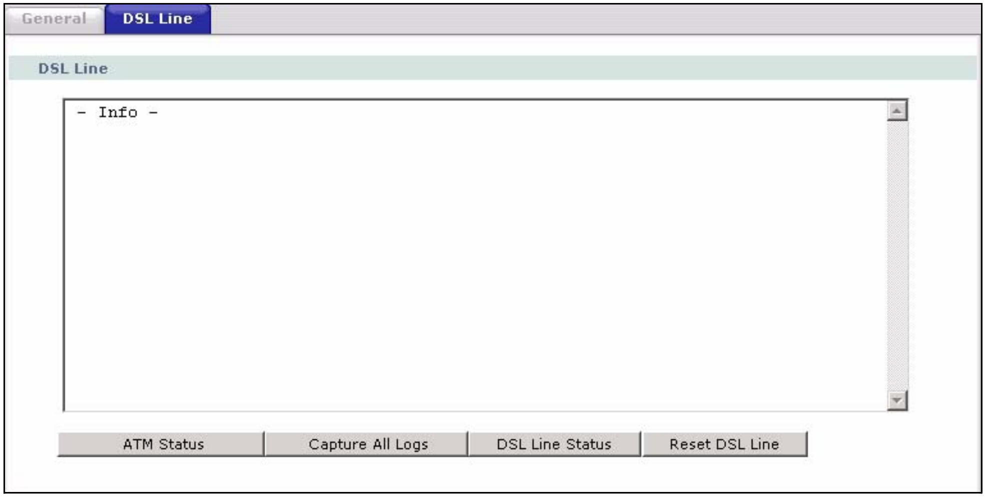
Table 49 Diagnostic > General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered. The results are displayed in the screen.

16.2 DSL Line Diagnostic

Use this screen to run DSL diagnostics. Click **Maintenance > Diagnostic > DSL Line** to open the screen shown next.

Figure 90 Diagnostic > DSL Line



The following table describes the fields in this screen.

Table 50 Diagnostic > DSL Line

LABEL	DESCRIPTION
ATM Status	Click this button to view ATM status.
Capture All Logs	Click this button to display all logs generated by the DSL line.
DSL Line Status	Click this button to view the DSL port's line operating values and line bit allocation.

Reset DSL Line	Click this button to reinitialize the DSL line. The large text box above then displays the progress and results of this operation, for example:
	`"Start to reset DSL`
	`Loading DSL modem F/W...`
	`Reset DSL Line Successfully!"`

PART VI
SMT and Troubleshooting

17

Introducing the SMT

The System Management Terminal (SMT) provides a text-based, menu-driven console to manage the ZyXEL Device. This chapter describes how to access the SMT and then provides an overview of its menus.

17.1 Accessing the SMT Via the Console Port

Use the CON/AUX port to configure the ZyXEL Device via SMT menus. Set the CON/AUX switch to CON (Console) side to use the CON/AUX port for local device configuration and management. Connect the RJ-45 connector of the console cable to the CON/AUX port of the ZyXEL Device and the other end to a serial port (COM1, COM2 or other COM port) on your computer. Your computer must have a terminal emulation communications program (such as HyperTerminal) set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no flow control and 9600 b/s port speed.

17.2 Accessing the SMT Via Telnet

Use Telnet to access the SMT. Use the yellow Ethernet cable to connect a computer to the ETHERNET port of the ZyXEL Device. Follow these steps.

1 In Windows, click **Start** > **Run**.

2 Type "telnet w.x.y.z", and click **OK**.
w.x.y.z is the IP address of the ZyXEL Device; the default address is 192.168.1.1.
The ZyXEL Device prompts you for the password.

Figure 91 Login Screen

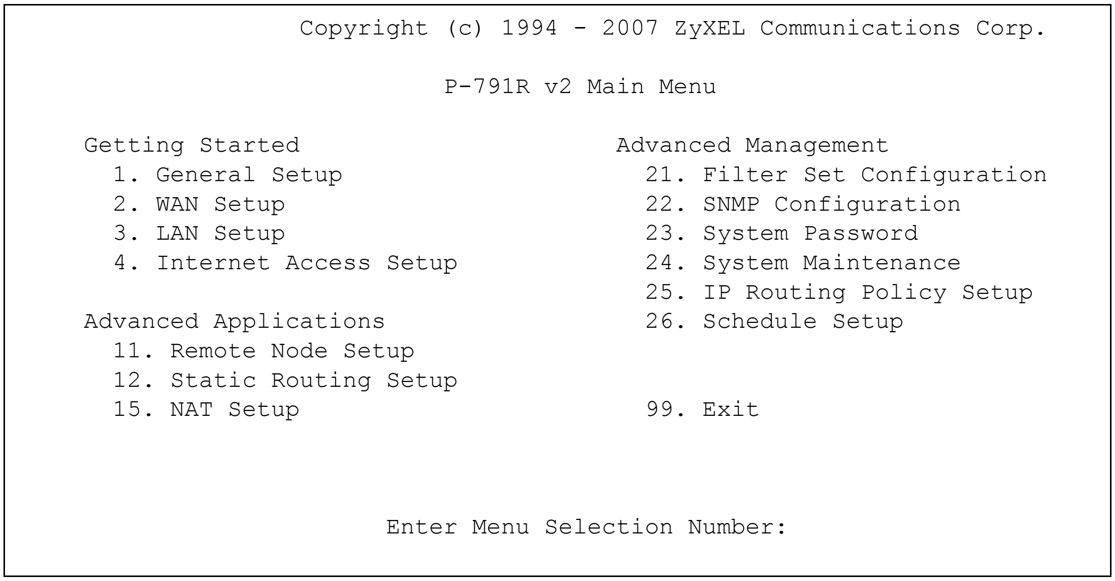
```
                    Password : xxxx
```

3 Enter the password. The default password is 1234. As you type the password, the screen displays an asterisk "*" for each character you type.

4 After you enter the password, the SMT main menu appears, as shown next.

Use menu 23.1 to change the password.

Figure 92 SMT Main Menu



```
                    Copyright (c) 1994 - 2007 ZyXEL Communications Corp.

                              P-791R v2 Main Menu

     Getting Started                    Advanced Management
       1. General Setup                   21. Filter Set Configuration
       2. WAN Setup                       22. SNMP Configuration
       3. LAN Setup                       23. System Password
       4. Internet Access Setup           24. System Maintenance
                                          25. IP Routing Policy Setup
     Advanced Applications                26. Schedule Setup
       11. Remote Node Setup
       12. Static Routing Setup
       15. NAT Setup                      99. Exit



                          Enter Menu Selection Number:
```

There is an inactivity timeout, and the default value is ten minutes. If there is no activity for longer than this, your ZyXEL Device will automatically log you out. You will then have to telnet into the ZyXEL Device again. You can use the web configurator or the CI commands (menu 24.8) to change the inactivity timeout period.

17.3 SMT Menu Items

The following table provides an overview of each menu item.

Table 51 Main Menu Summary

MENU	FUNCTION
1 General Setup	Use this menu to set up device mode, dynamic DNS and administrative information.
2 WAN Setup	Use this menu to configure the DSL connection, traffic redirect, and dial-backup interface.
3 LAN Setup	Use this to apply LAN filters, configure LAN DHCP and TCP/IP settings, and to allow or block layer-2 traffic between each pair of ports.
4 Internet Access Setup	Use this menu to configure your Internet connection.
11 Remote Node Setup	Use this menu to configure detailed remote node settings (for example, your ISP is a remote node) as well as apply filters.
12 Static Routing Setup	Use this menu to configure IP and bridge (MAC) static routes.
15 NAT Setup	Use this menu to configure Network Address Translation (NAT) on the ZyXEL Device.
21 Filter Set Configuration	Use this menu to configure filters.

Table 51 Main Menu Summary

MENU	FUNCTION
22 SNMP Configuration	Use this menu to configure SNMP.
23 System Password	Use this menu to change your password.
24 System Maintenance	Use this menu for comprehensive system maintenance, from looking at the system status to uploading firmware. You can also access the Command Interface (CI).
25 IP Routing Policy Setup	Use this menu to configure policy routes.
26 Schedule Setup	Use this menu to configure schedule sets.
99 Exit	Use this menu to exit the SMT.

The following table gives you an overview of the various SMT menus.

Table 52 SMT Menus Overview

MENUS	SUB MENUS		
1 General Setup	1.1 Configure Dynamic DNS		
2 WAN Setup	2.1 Traffic Redirect Setup		
	2.2 Dial Backup Setup	2.2.1 Advanced Dial Backup Setup	
3 LAN Setup	3.1 LAN Port Filter Setup		
	3.2 TCP/IP and DHCP Setup	3.2.1 IP Alias Setup	
4 Internet Access Setup			
11 Remote Node Setup	11.1 Remote Node Profile		
	11.3 Remote Node Network Layer Options		
	11.5 Remote Node Filter		
	11.6 Remote Node ATM Layer Options		
	11.8 Advance Setup Options		
12 Static Route Setup	12.1 IP Static Route Setup	12.1.1 Edit IP Static Route	
	12.3 Bridge Static Route Setup	12.3.1 Edit Bridge Static Route	
15 NAT Setup	15.1 Address Mapping Sets	15.1.x Address Mapping Rules	15.1.x.x Address Mapping Rule
	15.2 NAT Server Sets	15.2.x NAT Server Setup	
21 Filter Set Configuration	21.1 x Filter Rules Summary	21.1.x.x TCP/IP Filter Rule	
22 SNMP Configuration			
23 System Password			

Table 52 SMT Menus Overview (continued)

MENUS	SUB MENUS		
24 System Maintenance	24.1 System Maintenance - System Status		
	24.2 System Information and Console Port Speed	24.2.1 System Maintenance - Information	
		24.2.2 System Maintenance - Change Console Port Speed	
	24.3 System Maintenance - Log and Trace	24.3.1 View Error Log	
		24.3.2 System Maintenance - UNIX Syslog	
	24.4 System Maintenance - Diagnostic		
	24.5 Backup Configuration		
	24.6 Restore Configuration		
	24.7 System Maintenance - Upload Firmware	24.7.1 System Maintenance - Upload System Firmware	
		24.7.2 System Maintenance - Upload System Configuration File	
	24.8 Command Interpreter Mode		
	24.9 System Maintenance - Call Control	24.9.1 Budget Management	
	24.10 System Maintenance - Time and Date Setting		
	24.11 Remote Management Control		
25 IP Routing Policy Summary	25.1 IP Routing Policy Setup	25.1.1 IP Routing Policy	
26 Schedule Setup	26.1 Schedule Set Setup		

17.4 Navigating the SMT Interface

You should be familiar with the following operations before you try to use the SMT to modify the configuration.

Table 53 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a “hidden” menu	Press [SPACE BAR] to change **No** to **Yes** then press [ENTER].	Fields beginning with “Edit” lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] once to change **No** to **Yes**, then press [ENTER] to go to the “hidden” menu.

Table 53 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move the cursor	[ENTER] or [UP]/ [DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<?> or **ChangeMe**	All fields with the symbol <?> must be filled in order to be able to save the new configuration. All fields with **ChangeMe** must not be left blank in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message “Press ENTER to confirm or ESC to cancel”. Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

18

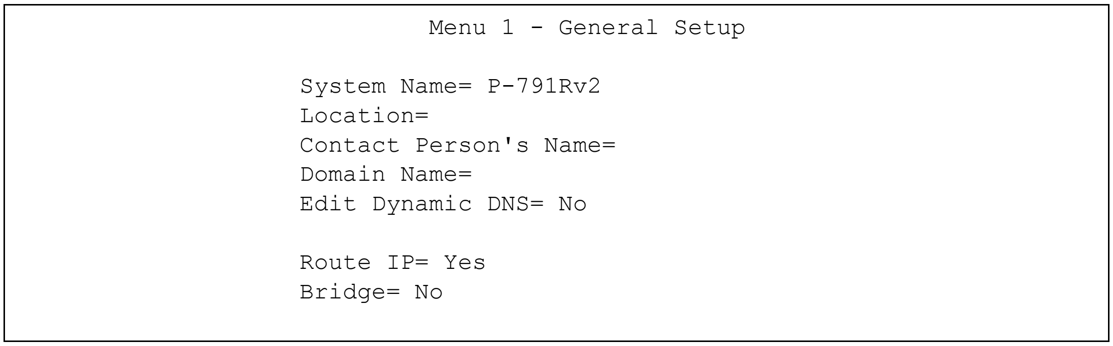
General Setup

Use this menu to set up device mode, dynamic DNS and administrative information.

18.1 Configuring General Setup

1. Enter 1 in the main menu to open **Menu 1 - General Setup**.
2. The **Menu 1 - General Setup** screen appears, as shown next. Fill in the required fields.

Figure 93 Menu 1: General Setup



```
                              Menu 1 - General Setup

                    System Name= P-791Rv2
                    Location=
                    Contact Person's Name=
                    Domain Name=
                    Edit Dynamic DNS= No

                    Route IP= Yes
                    Bridge= No
```

The following table describes the fields in this menu.

Table 54 Menu 1: General Setup

FIELD	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Location	Enter a descriptive name for the place where the ZyXEL Device is located. You can enter up to 31 characters, or you can leave this field blank.
Contact Person's Name	Enter the name of the person to contact for questions about the ZyXEL Device. You can enter up to 30 characters, or you can leave this field blank.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domain name" to see the current domain name used by your router. The domain name entered by you is given priority over the ISP assigned domain name. If you want to clear this field just press [SPACE BAR] and then [ENTER].
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1: Configure Dynamic DNS** discussed next.

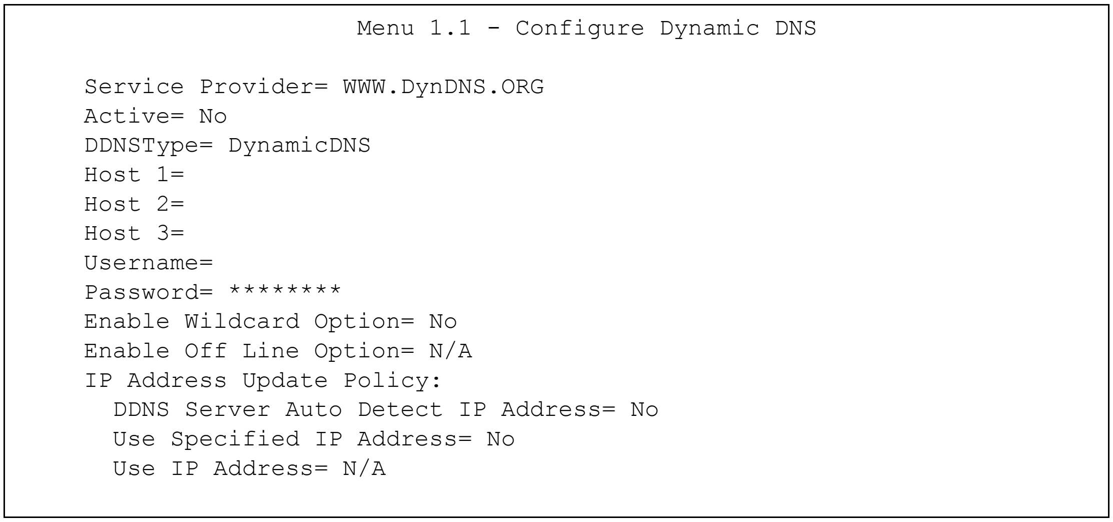
Table 54 Menu 1: General Setup (continued)

FIELD	DESCRIPTION
Route IP	Select **Yes** to enable IP-based routing in the ZyXEL Device. This is not effective for a specific remote node unless you enable IP-based routing in the remote node too. See Menu 11.1: Remote Node Profile (nodes 1-7) in Section 22.3 on page 185. You should enable **Route IP**, **Bridge**, or both in this screen. If you disable **Route IP** and **Bridge**, the device does not send traffic between the LAN ports and remote node.
Bridge	If **Route IP** is **Yes**, select **Yes** in this field to enable bridging in the ZyXEL Device for protocols that are not supported by IP-based routing (for example, SNA). If **Route IP** is **No**, select **Yes** in this field to enable bridging in the ZyXEL Device for all protocols. In either case, this setting is not effective for a specific remote node unless you enable bridging in the remote node too. See Menu 11.1: Remote Node Profile (nodes 1-7) in Section 22.3 on page 185. You should enable **Route IP**, **Bridge**, or both in this screen. If you disable **Route IP** and **Bridge**, the device does not send traffic between the LAN ports and remote node.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

18.1.1 Configuring Dynamic DNS

To configure Dynamic DNS, set the ZyXEL Device to router mode in menu 1 or in the **MAINTENANCE Device Mode** screen and go to **Menu 1 - General Setup** and press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1 - Configure Dynamic DNS** (shown next).

Figure 94 Menu 1.1: Configure Dynamic DNS



```
                    Menu 1.1 - Configure Dynamic DNS

     Service Provider= WWW.DynDNS.ORG
     Active= No
     DDNSType= DynamicDNS
     Host 1=
     Host 2=
     Host 3=
     Username=
     Password= ********
     Enable Wildcard Option= No
     Enable Off Line Option= N/A
     IP Address Update Policy:
       DDNS Server Auto Detect IP Address= No
       Use Specified IP Address= No
       Use IP Address= N/A
```

Follow the instructions in the next table to configure Dynamic DNS parameters.

Table 55 Menu 1.1: Configure Dynamic DNS

FIELD	DESCRIPTION
Service Provider	This is the name of your Dynamic DNS service provider.
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.
DDNSType	Press [SPACE BAR] and then [ENTER] to select **DynamicDNS** if you have the Dynamic DNS service. Select **StaticDNS** if you have the Static DNS service. Select **CustomDNS** if you have the Custom DNS service.
Host 1-3	Enter up to three host names in these fields.
Username	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Your ZyXEL Device supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. This field is **N/A** when you choose DDNS client as your service provider.
Enable Off Line Option	This field is only available when **CustomDNS** is selected in the **DDNS Type** field. Press [SPACE BAR] and then [ENTER] to select **Yes**. When **Yes** is selected, http://www.dyndns.org/ traffic is redirected to a URL that you have previously specified (see www.dyndns.org for details).
IP Address Update Policy:	You can select **Yes** in either the **DDNS Server Auto Detect IP Address** field (recommended) or the **Use Specified IP Address** field, but not both. With the **DDNS Server Auto Detect IP Address** and **Use Specified IP Address** fields both set to **No**, the DDNS server automatically updates the IP address of the host name(s) with the ZyXEL Device's WAN IP address. DDNS does not work with a private IP address. When both fields are set to **No**, the ZyXEL Device must have a public WAN IP address in order for DDNS to work.
DDNS Server Auto Detect IP Address	Only select this option when there are one or more **NAT** routers between the ZyXEL Device and the DDNS server. Press [SPACE BAR] to select **Yes** and then press [ENTER] to have the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyXEL Device and the DDNS server.
Use Specified IP Address	Press [SPACE BAR] to select **Yes** and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below. Only select **Yes** if the ZyXEL Device uses or is behind a static public IP address.
Use IP Address	Enter the static public IP address if you select **Yes** in the **Use Specified IP Address** field.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

19

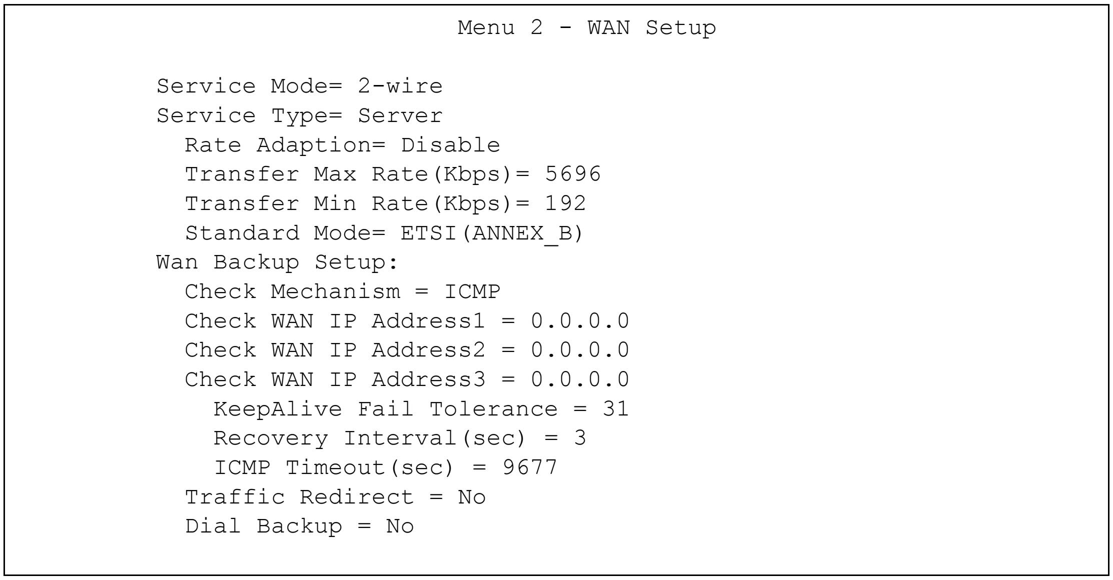
WAN Setup

Use this menu to configure the DSL connection, traffic redirect, and dial-backup interface.

19.1 WAN Setup

From the main menu, enter 2 to open menu 2.

Figure 95 Menu 2: WAN Setup



```
                              Menu 2 - WAN Setup

          Service Mode= 2-wire
          Service Type= Server
            Rate Adaption= Disable
            Transfer Max Rate(Kbps)= 5696
            Transfer Min Rate(Kbps)= 192
            Standard Mode= ETSI(ANNEX_B)
          Wan Backup Setup:
            Check Mechanism = ICMP
            Check WAN IP Address1 = 0.0.0.0
            Check WAN IP Address2 = 0.0.0.0
            Check WAN IP Address3 = 0.0.0.0
              KeepAlive Fail Tolerance = 31
              Recovery Interval(sec) = 3
              ICMP Timeout(sec) = 9677
            Traffic Redirect = No
            Dial Backup = No
```

The following table describes the fields in this screen.

Table 56 Menu 2: WAN Setup

FIELD	DESCRIPTION
Service Mode	This field indicates that the ZyXEL Device uses **2-wire** mode for the DSL connection. This is related to the phone line you use and affects the maximum speed of the connection. In **2-wire** mode, the maximum data rate is up to 5.69 Mbps.
Service Type	Press [SPACE BAR] to indicate whether the ZyXEL Device is the server or the client in the DSL connection. Select **Server** if this ZyXEL Device is the server in a point-to-point application. (See Chapter 4 on page 55.) Otherwise, select **Client**.
Rate Adaption	This field is configurable if **Service Type** is **Server**. Press [SPACE BAR] to let the ZyXEL Device adjust the speed of its connection to that of the other device.

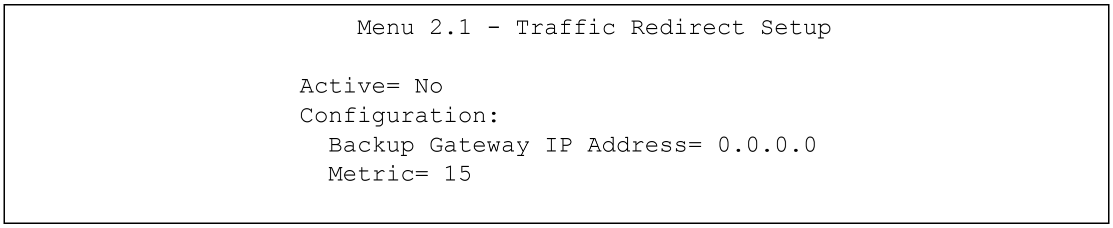
Table 56 Menu 2: WAN Setup (continued)

FIELD	DESCRIPTION
Transfer Max Rate(Kbps)	This field is enabled if **Service Type** is **Server**. Press [SPACE BAR] to set the maximum rate at which the ZyXEL Device sends and receives information. If you enable **Rate Adaption**, the ZyXEL Device adjusts to the speed of the other device and may exceed this rate.
Transfer Min Rate(Kbps)	This field is enabled if **Service Type** is **Server**. Press [SPACE BAR] to set the minimum rate at which the ZyXEL Device sends and receives information. If you enable **Rate Adaption**, the ZyXEL Device adjusts to the speed of the other device and may transfer information at less than this rate.
Standard Mode	This field is enabled if **Service Type** is **Server**. Press [SPACE BAR] to select the operational mode the ZyXEL Device uses in the DSL connection.
Wan Backup Setup	
Check Mechanism	Select the method that the ZyXEL Device uses to check the DSL connection. Select **DSL Link** to have the ZyXEL Device check if the connection to the DSLAM is up. Select **ICMP** to have the ZyXEL Device periodically ping the IP addresses configured in the **Check WAN IP Address** fields.
Check WAN IP Address1 Check WAN IP Address2 Check WAN IP Address3	Configure this field to test your ZyXEL Device's WAN accessibility. Type the IP address of up to three reliable, nearby computers (for example, your ISP's DNS server address). Note: If you activate either traffic redirect or dial backup, you must configure at least one IP address here. When using a WAN backup connection, the ZyXEL Device periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
KeepAlive Fail Tolerance	Type the number of times (2 recommended) that your ZyXEL Device may ping the IP addresses configured in the **Check WAN IP Address** field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval(sec)	When the ZyXEL Device is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the ZyXEL Device to wait between checks. Allow more time if your destination IP address handles lots of traffic.
ICMP Timeout(sec)	Type the number of seconds (3 recommended) for your ZyXEL Device to wait for a ping response from one of the IP addresses in the **Check WAN IP Address** field before timing out the request. The WAN connection is considered "down" after the ZyXEL Device times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	Press [SPACE BAR] to select **Yes** and then press [ENTER] to activate traffic redirect and to edit its settings.
Dial Backup	Press [SPACE BAR] to select **Yes** and then press [ENTER] to activate the dial-backup interface and to edit its settings.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

19.2 Configuring Traffic Redirect

From the main menu, in menu 2, select **Yes** in **Traffic Redirect**, and then press [ENTER].

Figure 96 Menu 2.1: Traffic Redirect Setup



```
                         Menu 2.1 - Traffic Redirect Setup

                     Active= No
                     Configuration:
                       Backup Gateway IP Address= 0.0.0.0
                       Metric= 15
```

The following table describes the fields in this menu.

Table 57 Menu 2.1: Traffic Redirect Setup

FIELD	DESCRIPTION
Active	Use this field to turn the traffic redirect feature on (**Yes**) or off (**No**).
Configuration	
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The ZyXEL Device automatically forwards traffic to this IP address if the ZyXEL Device's Internet connection terminates.
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

19.3 Dial Backup Interface

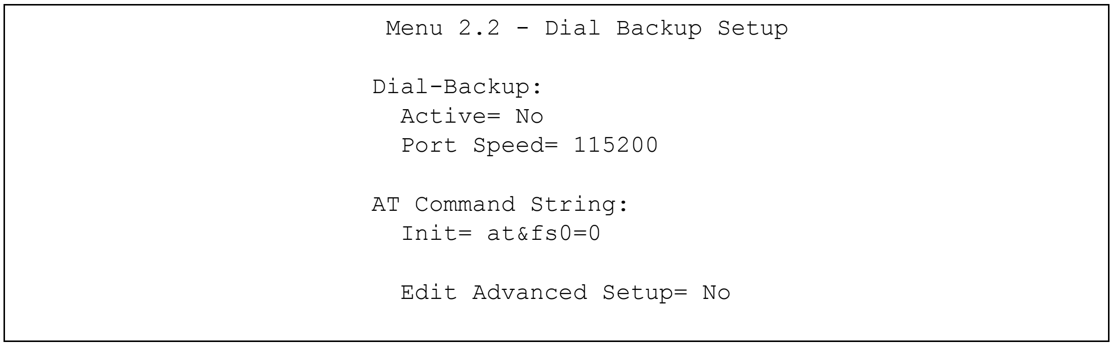
In the SMT, to set up the auxiliary port for use, first make sure you have set up the switch and port connection. Then, use the following menus.

1. Menu 2 - WAN Setup
2. Menu 2.2 - Dial Backup Setup
3. Menu 2.2.1 - Advanced Dial Backup Setup and
4. Menu 11.1 - Remote Node Profile (node 8, Backup ISP)

19.4 Configuring Dial Backup in Menu 2

From the main menu, enter 2 to open menu 2.

Figure 97 Menu 2.2: Dial Backup Setup



```
                    Menu 2.2 - Dial Backup Setup

                   Dial-Backup:
                     Active= No
                     Port Speed= 115200

                   AT Command String:
                     Init= at&fs0=0

                     Edit Advanced Setup= No
```

The following table describes the fields in this menu.

Table 58 Menu 2.2: Dial Backup Setup

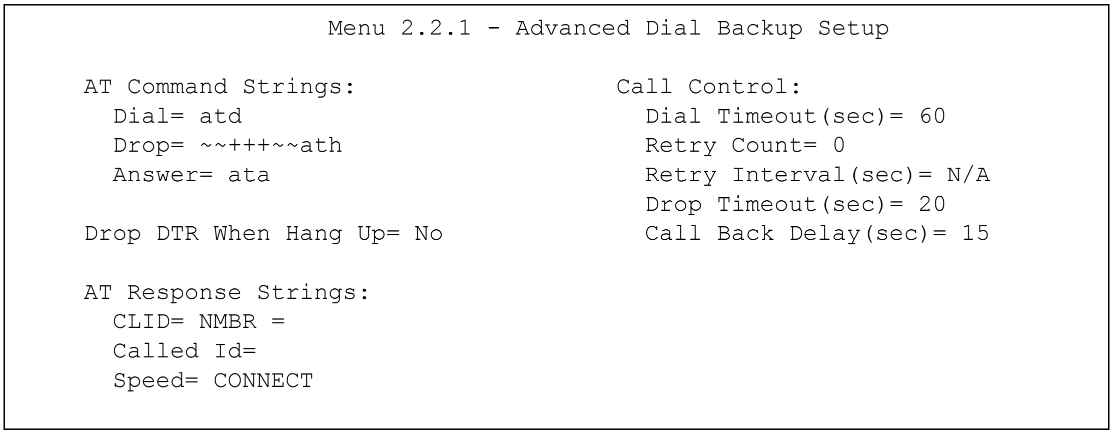
FIELD	DESCRIPTION
Dial-Backup:	
Active	Use this field to turn the dial-backup feature on (**Yes**) or off (**No**).
Port Speed	Press [SPACE BAR] and then press [ENTER] to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: **9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps.
AT Command String:	
Init	Enter the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.
Edit Advanced Setup	To edit the advanced setup for the Dial Backup port, move the cursor to this field; press the [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 2.1 - Advanced Setup**.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

19.5 Advanced Dial Backup Setup

Consult the manual of the device connected to your Dial Backup port for specific AT commands.

To edit the advanced setup for the Dial Backup port, move the cursor to the **Edit Advanced Setup** field in **Menu 2.2 - Dial Backup Setup**, press the [SPACE BAR] to select **Yes** and then press [ENTER].

Figure 98 Menu 2.2.1: Advanced Dial Backup Setup



```
                    Menu 2.2.1 - Advanced Dial Backup Setup

     AT Command Strings:                    Call Control:
       Dial= atd                              Dial Timeout(sec)= 60
       Drop= ~~+++~~ath                       Retry Count= 0
       Answer= ata                            Retry Interval(sec)= N/A
                                              Drop Timeout(sec)= 20
     Drop DTR When Hang Up= No                Call Back Delay(sec)= 15

     AT Response Strings:
       CLID= NMBR =
       Called Id=
       Speed= CONNECT
```

The following table describes fields in this menu.

Table 59 Menu 2.2.1: Advanced Dial Backup Setup

FIELD	DESCRIPTION
AT Command Strings:	
Dial	Enter the AT Command string to make a call.
Drop	Enter the AT Command string to drop a call. “~” represents a one second wait, for example “~~~+++~~ath” can be used if your modem has a slow response time.
Answer	Enter the AT Command string to answer a call.
Drop DTR When Hang Up	Press the [SPACE BAR] to choose either **Yes** or **No**. When **Yes** is selected (the default), the DTR (Data Terminal Ready) signal is dropped after the “AT Command String: Drop” is sent out.
AT Response Strings:	
CLID (Calling Line Identification)	Enter the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyXEL Device capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.
Called Id	Enter the keyword preceding the dialed number.
Speed	Enter the keyword preceding the connection speed.
Call Control	
Dial Timeout (sec)	Enter a number of seconds for the ZyXEL Device to keep trying to set up an outgoing call before timing out (stopping). The ZyXEL Device times out and stops if it cannot set up an outgoing call within the timeout value.
Retry Count	Enter a number of times for the ZyXEL Device to retry a busy or no-answer phone number before blacklisting the number.
Retry Interval (sec)	Enter a number of seconds for the ZyXEL Device to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.
Drop Timeout (sec)	Enter a number of seconds for the ZyXEL Device to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.
Call Back Delay (sec)	Enter a number of seconds for the ZyXEL Device to wait between dropping a callback request call and dialing the corresponding callback call.

20

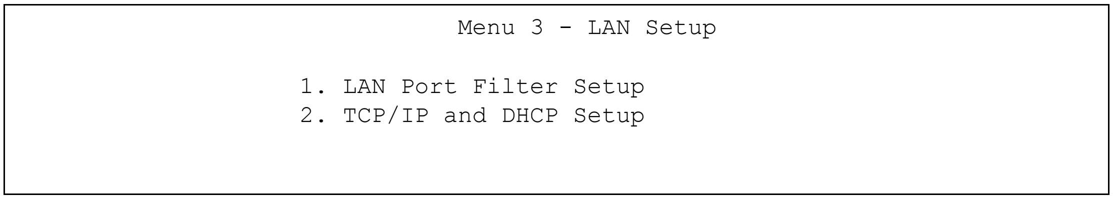
LAN Setup

Use this to apply LAN filters, configure LAN DHCP and TCP/IP settings, and to activate or deactivate VLAN on each LAN port.

20.1 Accessing the LAN Menus

From the main menu, enter 3 to open **Menu 3 - LAN Setup**.

Figure 99 Menu 3: LAN Setup

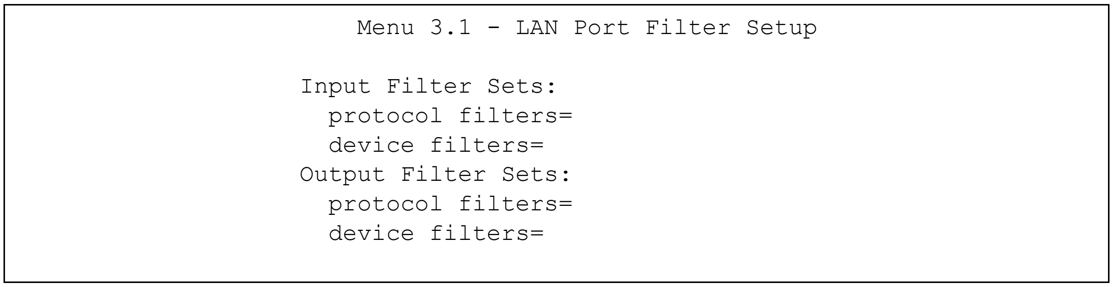


```
                          Menu 3 - LAN Setup

                     1. LAN Port Filter Setup
                     2. TCP/IP and DHCP Setup
```

20.2 LAN Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to the LAN traffic. You seldom need to filter the LAN traffic, however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

Figure 100 Menu 3.1: LAN Port Filter Setup

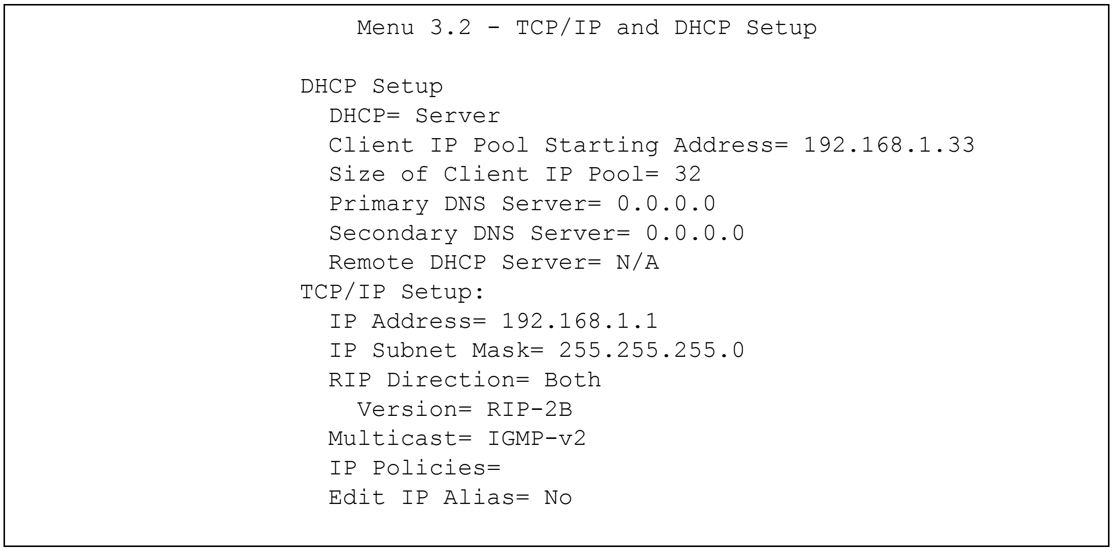


```
                       Menu 3.1 - LAN Port Filter Setup

                   Input Filter Sets:
                     protocol filters=
                     device filters=
                   Output Filter Sets:
                     protocol filters=
                     device filters=
```

20.3 TCP/IP and DHCP Setup Menu

From the main menu, enter 3 to open **Menu 3 - LAN Setup** to configure TCP/IP (RFC 1155) and DHCP setup. From menu 3, select the submenu option **TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 3.2 - TCP/IP and DHCP Ethernet Setup,** as shown next. Not all fields are available on all models.

Figure 101 Menu 3.2: TCP/IP and DHCP Ethernet Setup



```
                              Menu 3.2 - TCP/IP and DHCP Setup

                          DHCP Setup
                            DHCP= Server
                            Client IP Pool Starting Address= 192.168.1.33
                            Size of Client IP Pool= 32
                            Primary DNS Server= 0.0.0.0
                            Secondary DNS Server= 0.0.0.0
                            Remote DHCP Server= N/A
                          TCP/IP Setup:
                            IP Address= 192.168.1.1
                            IP Subnet Mask= 255.255.255.0
                            RIP Direction= Both
                              Version= RIP-2B
                            Multicast= IGMP-v2
                            IP Policies=
                            Edit IP Alias= No
```

Follow the instructions in the next table to configure these fields.

Table 60 Menu 3.2: TCP/IP and DHCP Ethernet Setup

FIELD	DESCRIPTION
DHCP Setup	
DHCP	This field enables/disables the DHCP server. If set to **Server**, your ZyXEL Device will act as a DHCP server. You should configure the rest of the fields in this section except for **Remote DHCP Server**. If set to **Relay**, the ZyXEL Device acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients. The **Remote DHCP Server** needs to be set. If set to **None**, the DHCP server will be disabled.
Client IP Pool Starting Address:	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.

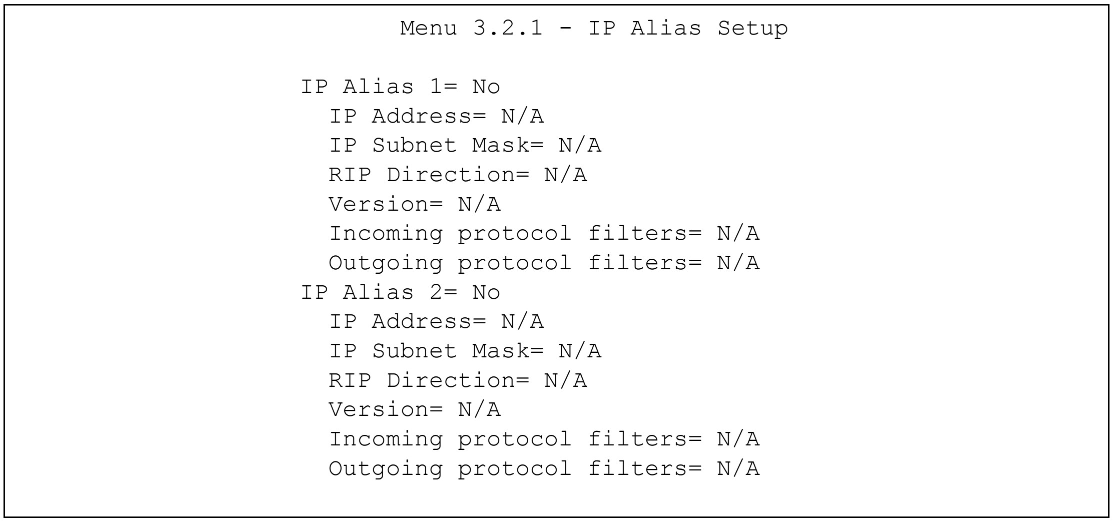
Table 60 Menu 3.2: TCP/IP and DHCP Ethernet Setup (continued)

FIELD	DESCRIPTION
Primary DNS Server Secondary DNS Server	The ZyXEL Device passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. Select **From ISP** if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). The **IP Address** field below displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the **IP Address** field below. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you save your changes. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you save your changes. Select **DNS Relay** to have the ZyXEL Device act as a DNS proxy. The ZyXEL Device's LAN IP address displays in the I**P Address** field below (read-only). The ZyXEL Device tells the DHCP clients on the LAN that the ZyXEL Device itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyXEL Device, the ZyXEL Device forwards the query to the ZyXEL Device's system DNS server (configured in menu 1) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you save your changes. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above, then type the IP address of the actual remote DHCP server here.
TCP/IP Setup:	
IP Address	Enter the LAN IP address of your ZyXEL Device in dotted decimal notation
IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: **Both**, **In Only**, **Out Only** or **None**.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: **RIP-1**, **RIP-2B** or **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyXEL Device supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press [SPACE BAR] and then [ENTER] to enable IP Multicasting or select **None** (default) to disable it.
IP Policies	You can apply up to four policy routes for this remote node. Configure the policy routes in menu 25 first. See Chapter 31 on page 261 for information about policy routes.
Edit IP Alias	The ZyXEL Device supports three logical LAN interfaces via its single physical Ethernet interface with the ZyXEL Device itself as the gateway for each LAN network. Press [SPACE BAR] to select **Yes** and then press [ENTER] to display menu 3.2.1.
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.	

20.4 LAN IP Alias

Use menu 3.2 to configure the first network, and you use menu 3.2.1 to configure the other two networks. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Figure 102 Menu 3.2.1: IP Alias Setup



```
                          Menu 3.2.1 - IP Alias Setup

                   IP Alias 1= No
                     IP Address= N/A
                     IP Subnet Mask= N/A
                     RIP Direction= N/A
                     Version= N/A
                     Incoming protocol filters= N/A
                     Outgoing protocol filters= N/A
                   IP Alias 2= No
                     IP Address= N/A
                     IP Subnet Mask= N/A
                     RIP Direction= N/A
                     Version= N/A
                     Incoming protocol filters= N/A
                     Outgoing protocol filters= N/A
```

Use the instructions in the following table to configure IP alias parameters.

Table 61 Menu 3.2.1: IP Alias Setup

FIELD	DESCRIPTION
IP Alias 1, 2	Choose **Yes** to configure the LAN network for the ZyXEL Device.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation.
IP Subnet Mask	Your ZyXEL Device will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyXEL Device.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are **Both**, **In Only**, **Out Only** or **None**.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.
Incoming protocol filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the ZyXEL Device.
Outgoing protocol filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the ZyXEL Device.
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.	

21

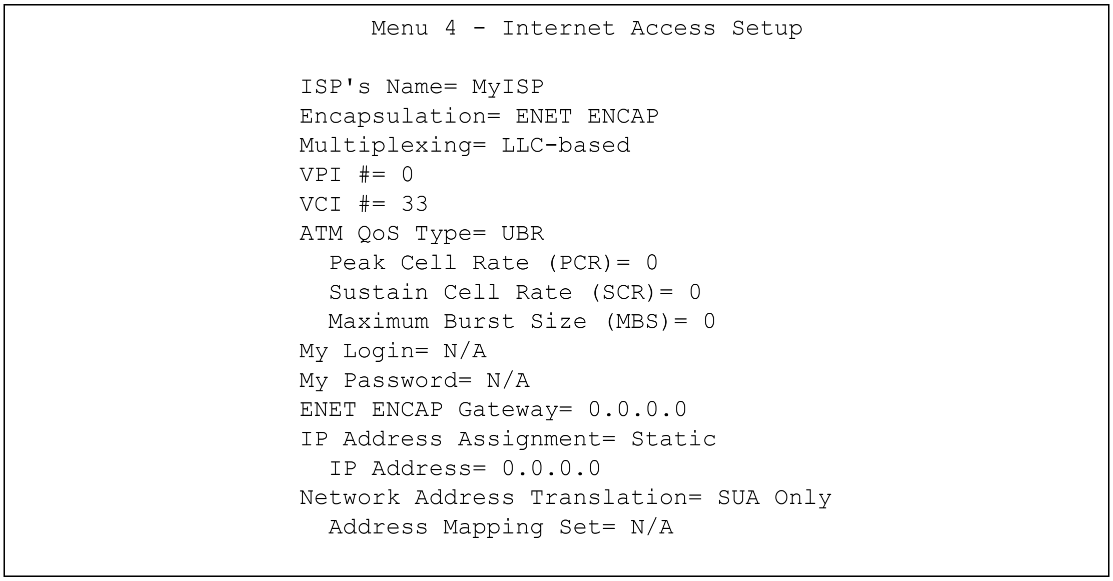
Internet Access Setup

Use this menu to configure your Internet connection. Use information from your ISP along with the instructions in this chapter to set up your ZyXEL Device to access the Internet. Contact your ISP to determine what encapsulation type you should use.

21.1 Internet Access Setup

Enter 4 in the main menu.

Figure 103 Menu 4: Internet Access Setup



```
                    Menu 4 - Internet Access Setup

               ISP's Name= MyISP
               Encapsulation= ENET ENCAP
               Multiplexing= LLC-based
               VPI #= 0
               VCI #= 33
               ATM QoS Type= UBR
                 Peak Cell Rate (PCR)= 0
                 Sustain Cell Rate (SCR)= 0
                 Maximum Burst Size (MBS)= 0
               My Login= N/A
               My Password= N/A
               ENET ENCAP Gateway= 0.0.0.0
               IP Address Assignment= Static
                 IP Address= 0.0.0.0
               Network Address Translation= SUA Only
                 Address Mapping Set= N/A
```

The following table describes the fields in this menu.

Table 62 Menu 4: Internet Access Setup

FIELD	DESCRIPTION
ISP's Name	Enter a descriptive name for your ISP for identification purposes.
Encapsulation	Press [SPACE BAR] and then press [ENTER] to select the type of encapsulation your ISP uses.
Multiplexing	Press [SPACE BAR] to select the method of multiplexing used by your ISP. Choices are **VC-based** or **LLC-based**.
VPI	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.

Table 62 Menu 4: Internet Access Setup (continued)

FIELD	DESCRIPTION
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
ATM QoS Type	Select **CBR** (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate (PCR)	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate (SCR)	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size (MBS)	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
My Login	(PPPoE and PPPoA only) Enter the login name given to you by your ISP.
My Password	(PPPoE and PPPoA only) Type your password again for confirmation.
ENET ENCAP Gateway	(ENET ENCAP only) Enter the gateway IP address provided by your ISP.
Idle Timeout (sec)	(PPPoE and PPPoA only) Specify an idle time-out. The default setting is 0, which means the Internet session will not timeout.
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**, otherwise select **Static** and enter the IP address and subnet mask in the following fields.
IP Address	This field is enabled if the **IP Address Assignment** is **Static**. Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field).
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose **None** to disable NAT. Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set. Please see Chapter 7 on page 93 for a more detailed discussion on the Network Address Translation feature.
Address Mapping Set	This field is enabled if the **Network Address Translation** is **Full Feature**. Enter the number of the address mapping set you want to use for your Internet connection.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

22

Remote Node Setup

Use this menu to configure detailed remote node settings (for example, your ISP is a remote node) as well as apply filters.

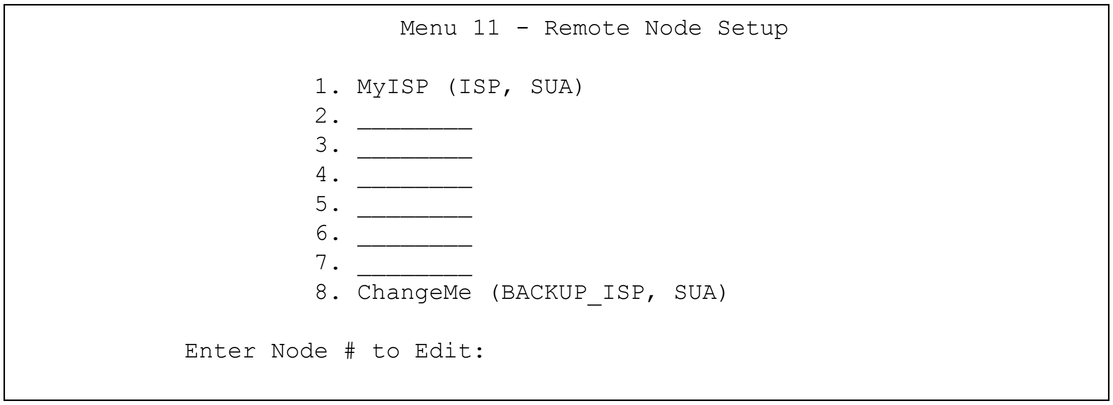
22.1 Introduction to Remote Node Setup

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node.

22.2 Remote Node Setup

From the main menu, select menu option 11 to open **Menu 11 - Remote Node Setup** (shown below).

Figure 104 Menu 11: Remote Node Setup



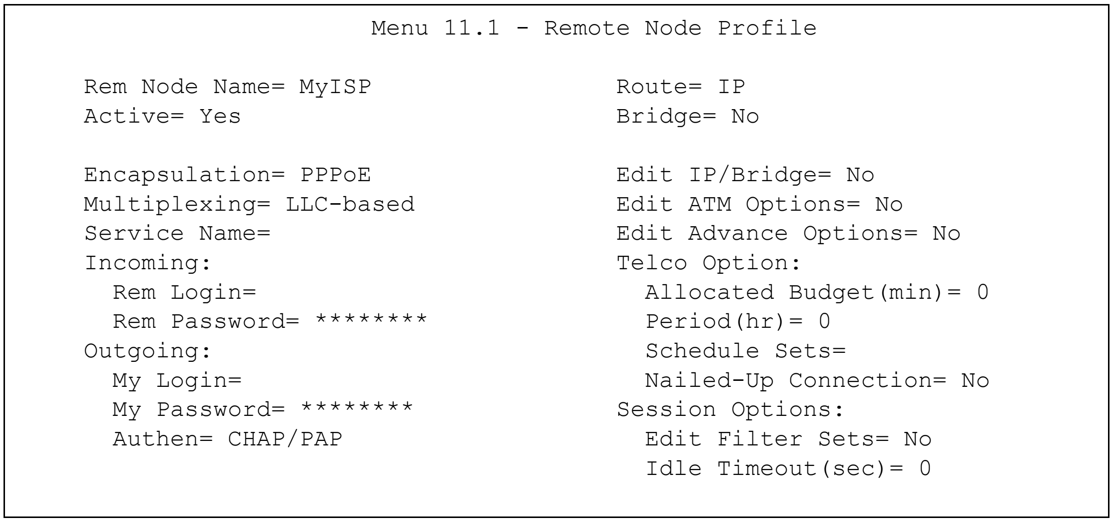
```
                              Menu 11 - Remote Node Setup

                         1. MyISP (ISP, SUA)
                         2. ________
                         3. ________
                         4. ________
                         5. ________
                         6. ________
                         7. ________
                         8. ChangeMe (BACKUP_ISP, SUA)

                Enter Node # to Edit:
```

Type the node number you want to configure and press [ENTER].

22.3 Remote Node Profile

The following explains how to configure remote nodes 1-7.

Figure 105 Menu 11.1: Remote Node Profile (nodes 1-7)



```
                      Menu 11.1 - Remote Node Profile

    Rem Node Name= MyISP                  Route= IP
    Active= Yes                           Bridge= No

    Encapsulation= PPPoE                  Edit IP/Bridge= No
    Multiplexing= LLC-based               Edit ATM Options= No
    Service Name=                         Edit Advance Options= No
    Incoming:                             Telco Option:
      Rem Login=                            Allocated Budget(min)= 0
      Rem Password= ********                Period(hr)= 0
    Outgoing:                               Schedule Sets=
      My Login=                             Nailed-Up Connection= No
      My Password= ********               Session Options:
      Authen= CHAP/PAP                      Edit Filter Sets= No
                                            Idle Timeout(sec)= 0
```

The following table describes the labels in this menu.

Table 63 Menu 11.1: Remote Node Profile (nodes 1-7)

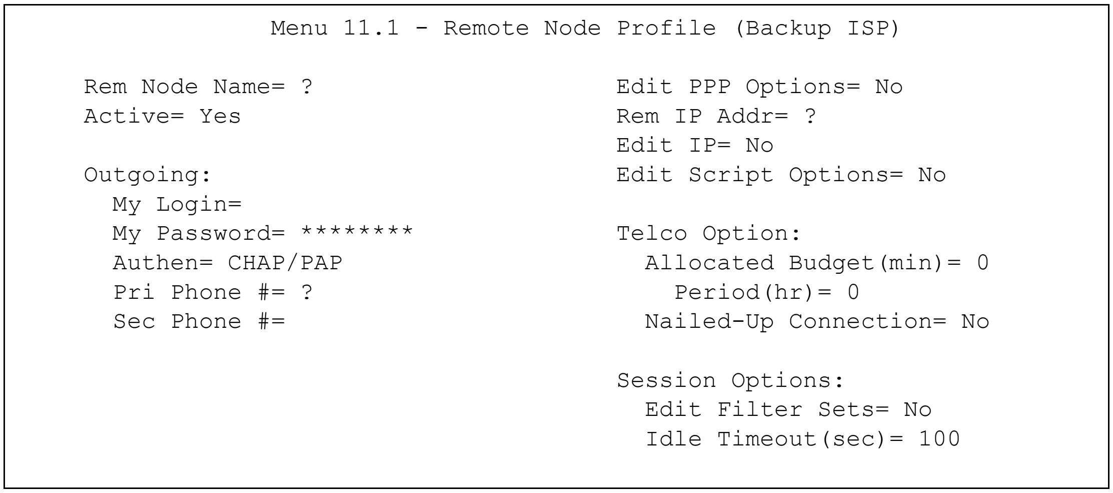
FIELD	DESCRIPTION
Rem Node Name	Enter the name of the ISP.
Active	Select whether or not you want to use this Internet connection.
Encapsulation	Select the type of encapsulation your ISP uses.
Multiplexing	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**.
Service Name	(PPPoE only) Enter the service name provided by your ISP. Leave this field blank if your ISP did not provide one.
Incoming	This section is only enabled for PPPoA or PPPoE connections.
Rem Login	Type the login name that this remote node will use to call your ZyXEL Device. The login name and the **Rem Password** will be used to authenticate this node.
Rem Password	Type the password used when this remote node calls your ZyXEL Device.
Outgoing	This section is only enabled for PPPoA or PPPoE connections.
My Login	Enter the user name provided by your ISP.
My Password	Enter the password provided by your ISP.
Retype to Confirm	Enter the password again.
Authen	This field appears if you select **PPPoE** in the **Encapsulation** field. Select what type of authentication your ISP uses. Select **CHAP/PAP** if you want the ZyXEL Device to support both choices.
Route	Press [SPACE BAR] and then [ENTER] to select **IP** to enable IP-based routing to this remote node. This is not effective unless you enable IP-based routing in the ZyXEL Device too. See Menu 1: General Setup in Section 18.1 on page 169. You should enable **Route IP**, **Bridge**, or both in this screen. If you disable **Route IP** and **Bridge**, the device does not send traffic between the LAN ports and remote node.

Table 63 Menu 11.1: Remote Node Profile (nodes 1-7) (continued)

FIELD	DESCRIPTION
Bridge	If **Route** is **IP**, select **Yes** in this field to enable bridging to this remote node for protocols that are not supported by IP-based routing (for example, SNA). If **Route** is **None**, select **Yes** in this field to enable bridging to this remote node for all protocols. In either case, this setting is not effective unless you enable bridging in the ZyXEL Device too. See Menu 1: General Setup in Section 18.1 on page 169. You should enable **Route IP**, **Bridge**, or both in this screen. If you disable **Route IP** and **Bridge**, the device does not send traffic between the LAN ports and remote node.
Edit IP/Bridge	This field is enabled if **Route** is **IP**. If you want to set up the WAN IP address and advanced features for the WAN port, press [SPACE BAR] to select **Yes** and press [ENTER]. Menu 11.3 appears.
Edit ATM Options	This field is enabled if **Route** is **IP**. Press [SPACE BAR] to select **Yes** and press [ENTER] to edit the virtual channel and ATM QoS settings. Menu 11.6 appears.
Edit Advance Options	This field is displayed if you are editing remote node 1, and it is only enabled for PPPoE connections. If you want to set up advanced features for the Internet connection, press [SPACE BAR] to select **Yes** and press [ENTER]. Menu 11.8 appears.
Telco Option	This section is only enabled for PPPoA or PPPoE connections.
Allocated Budget(min)	Enter the maximum amount of time (in minutes) each call can last. Enter 0 if there is no limit. With **Period**, you can set a limit on the total outgoing call time of the ZyXEL Device within a certain period of time. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.
Period(hr)	Enter how often (in hours) the **Allocated Budget** is reset. For example, if you can call for thirty minutes every hour, set the **Allocated Budget** to 30, and set this field to 1.
Schedule Sets	Enter the schedule sets that apply to this connection.
Nailed-Up Connection	Select this if you want the ZyXEL Device to automatically connect to your ISP when it is turned on and to remain connected all the time. This is not recommended if you pay for your Internet connected based on the amount of time you are connected.
Session Options	
Edit Filter Sets	If you want to specify input and output filter sets for the WAN port, press [SPACE BAR] to select **Yes** and press [ENTER]. Menu 11.5 appears.
Idle Timeout(sec)	Enter the number of seconds the ZyXEL Device should wait while there is no Internet traffic before it automatically disconnects from the ISP. Enter a time interval between 10 and 9999 seconds.

The following explains how to configure remote node 8 for the dial backup connection.

Figure 106 Menu 11.1: Remote Node Profile (node 8)



```
             Menu 11.1 - Remote Node Profile (Backup ISP)

Rem Node Name= ?                     Edit PPP Options= No
Active= Yes                          Rem IP Addr= ?
                                     Edit IP= No
Outgoing:                            Edit Script Options= No
  My Login=
  My Password= ********              Telco Option:
  Authen= CHAP/PAP                     Allocated Budget(min)= 0
  Pri Phone #= ?                         Period(hr)= 0
  Sec Phone #=                         Nailed-Up Connection= No

                                     Session Options:
                                       Edit Filter Sets= No
                                       Idle Timeout(sec)= 100
```

The following table describes the labels in this menu.

Table 64 Menu 11.1: Remote Node Profile (node 8)

FIELD	DESCRIPTION
Rem Node Name	Enter the name of the ISP.
Active	Select whether or not you want to use this Internet connection.
Outgoing	This section is only enabled for PPPoA or PPPoE connections.
My Login	Enter the user name provided by your ISP.
My Password	Enter the password provided by your ISP.
Retype to Confirm	Enter the password again.
Authen	This field appears if you select **PPPoE** in the **Encapsulation** field. Select what type of authentication your ISP uses. Select **CHAP/PAP** if you want the ZyXEL Device to support both choices.
Pri Phone # Sec Phone #	Type the phone number(s) for this remote node. If the Primary Phone number is busy or does not answer, your ZyXEL Device dials the Secondary Phone number, if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Edit PPP Options	Press [SPACE BAR] to select **Yes** and press [ENTER] to configure the PPP settings for the backup ISP. Menu 11.2 appears.
Rem IP Addr	This field displays the type of routing the ZyXEL Device uses.
Edit IP/Bridge	This field is enabled if **Route** is **IP**. If you want to set up the WAN IP address and advanced features for the WAN port, press [SPACE BAR] to select **Yes** and press [ENTER]. Menu 11.3 appears.
Edit ATM Options	This field is enabled if **Route** is **IP**. Press [SPACE BAR] to select **Yes** and press [ENTER] to edit the virtual channel and ATM QoS settings. Menu 11.6 appears.
Edit Advance Options	This field is displayed if you are editing remote node 1, and it is only enabled for PPPoE connections. If you want to set up advanced features for the Internet connection, press [SPACE BAR] to select **Yes** and press [ENTER]. Menu 11.8 appears.
Telco Option	This section is only enabled for PPPoA or PPPoE connections.

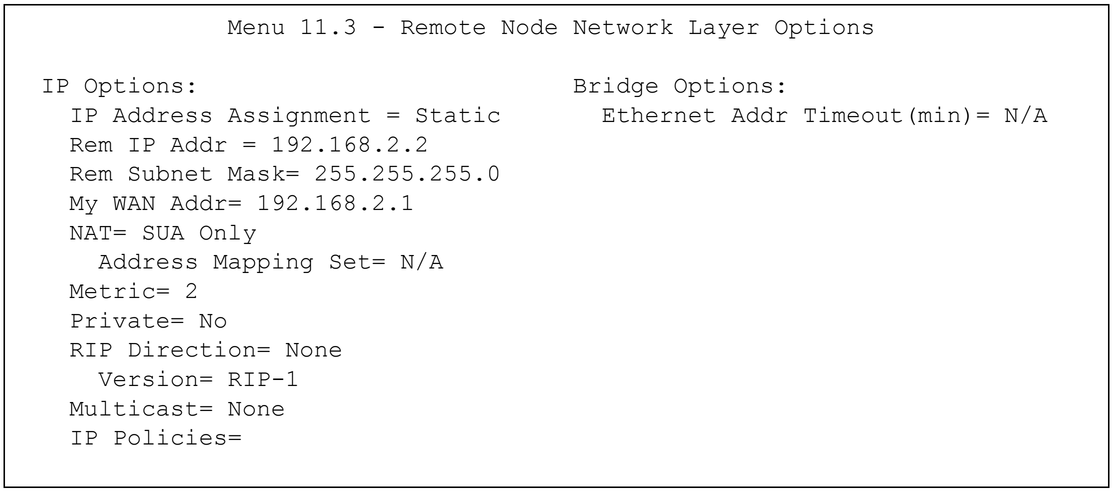
Table 64 Menu 11.1: Remote Node Profile (node 8) (continued)

FIELD	DESCRIPTION
Allocated Budget(min)	Enter the maximum amount of time (in minutes) each call can last. Enter 0 if there is no limit. With **Period**, you can set a limit on the total outgoing call time of the ZyXEL Device within a certain period of time. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.
Period(hr)	Enter how often (in hours) the **Allocated Budget** is reset. For example, if you can call for thirty minutes every hour, set the **Allocated Budget** to 30, and set this field to 1.
Schedule Sets	Enter the schedule sets that apply to this connection.
Nailed-Up Connection	Select this if you want the ZyXEL Device to automatically connect to your ISP when it is turned on and to remain connected all the time. This is not recommended if you pay for your Internet connected based on the amount of time you are connected.
Session Options	
Edit Filter Sets	If you want to specify input and output filter sets for the WAN port, press [SPACE BAR] to select **Yes** and press [ENTER]. Menu 11.5 appears.
Idle Timeout(sec)	Enter the number of seconds the ZyXEL Device should wait while there is no Internet traffic before it automatically disconnects from the ISP. Enter a time interval between 10 and 9999 seconds.

22.4 Remote Node Network Layer Options

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Remote Node Network Layer Options**.

Figure 107 Menu 11.3: Remote Node Network Layer Options



```
             Menu 11.3 - Remote Node Network Layer Options

 IP Options:                             Bridge Options:
   IP Address Assignment = Static          Ethernet Addr Timeout(min)= N/A
   Rem IP Addr = 192.168.2.2
   Rem Subnet Mask= 255.255.255.0
   My WAN Addr= 192.168.2.1
   NAT= SUA Only
     Address Mapping Set= N/A
   Metric= 2
   Private= No
   RIP Direction= None
     Version= RIP-1
   Multicast= None
   IP Policies=
```

The following table describes the fields in this menu.

Table 65 Menu 11.3: Remote Node Network Layer Options

FIELD	DESCRIPTION
IP Address Assignment	Select **Dynamic** if your ISP did not give you a fixed (static) IP address. Select **Static** if your ISP gave you a fixed (static) IP address. The next three fields are not available if you select **Dynamic**.
	These fields appear if you selected **Ethernet** in **Encapsulation** in menu 11.
Rem IP Address	If you have a static IP Assignment, enter the IP address assigned to you by your ISP.
Rem IP Subnet Mask	If you have a static IP Assignment, enter the subnet mask assigned to you.
My WAN Addr	Enter the fixed (static) IP address provided by your ISP.
NAT	Select **None** if you do not want to use port forwarding, trigger ports, or NAT. Select **SUA Only** if you want to use one or more of these features and have only one WAN IP address for your ZyXEL Device. Select **Full Feature** if you want to use one or more of these features and have more than one public WAN IP address for your ZyXEL Device.
Address Mapping Set	This field is enabled if **NAT** is **Full Feature**. Specify which address mapping set you want to use for this remote node.
Metric	This field sets this route's priority among the routes the ZyXEL Device uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Private	This field is related to RIP. This field determines whether or not the ZyXEL Device includes the route to this remote node in its RIP broadcasts. If you select **Yes**, this route is not included in RIP broadcast. If you select **No**, the route to this remote node is propagated to other hosts through RIP broadcasts. Usually, you should keep the default value.
RIP Direction	Use this field to control how much routing information the ZyXEL Device sends and receives through this connection. **None** - The ZyXEL Device does not send or receive routing information through this connection. **Both** - The ZyXEL Device sends and receives routing information through this connection. **In Only** - The ZyXEL Device only receives routing information through this connection. **Out Only** - The ZyXEL Device only sends routing information through this connection.
Version	Select which version of RIP the ZyXEL Device uses when it sends or receives information on the subnet. **RIP-1** - The ZyXEL Device uses RIPv1 to exchange routing information. **RIP-2B** - The ZyXEL Device broadcasts RIPv2 to exchange routing information. **RIP-2M** - The ZyXEL Device multicasts RIPv2 to exchange routing information.

Table 65 Menu 11.3: Remote Node Network Layer Options (continued)

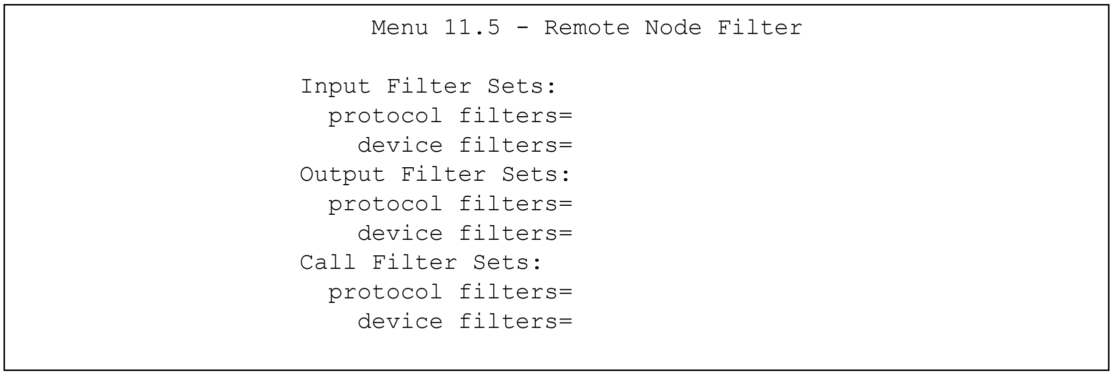
FIELD	DESCRIPTION
Multicast	You do not have to enable multicasting to use **RIP-2M**. (See **RIP Version**.) Select which version of IGMP the ZyXEL Device uses to support multicasting on this port. Multicasting only sends packets to some computers and is an alternative to unicasting (sending packets to one computer) and broadcasting (sending packets to every computer). **None** - The ZyXEL Device does not support multicasting. **IGMP-v1** - The ZyXEL Device supports IGMP version 1. **IGMP-v2** - The ZyXEL Device supports IGMP version 2. Multicasting can improve overall network performance. However, it requires extra processing and generates more network traffic. In addition, other computers have to support the same version of IGMP.
IP Policies	You can apply up to four policy routes for this remote node. Configure the policy routes in menu 25 first. See Chapter 31 on page 261 for information about policy routes.
Bridge Options	
Ethernet Addr Timeout(min)	This field is enabled if **Bridge** is **Yes** in SMT Menu 11.1: Remote Node Profile (nodes 1-7). Type the time (in minutes) for the ZyXEL Device to retain the Ethernet address information in its internal tables while the line is down. If this information is retained, your ZyXEL Device will not have to recompile the tables when the line comes back up.
Once you have completed filling in this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration and return to menu 11.1, or press [ESC] at any time to cancel.	

22.5 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.5 - Remote Node Filter**.

Use this menu to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyXEL Device to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For more information on defining the filters, please refer to Chapter 25 on page 213. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

Figure 108 Menu 11.5: Remote Node Filter



```
                  Menu 11.5 - Remote Node Filter

             Input Filter Sets:
               protocol filters=
                 device filters=
             Output Filter Sets:
               protocol filters=
                 device filters=
             Call Filter Sets:
               protocol filters=
                 device filters=
```

The following table describes the labels in this menu.

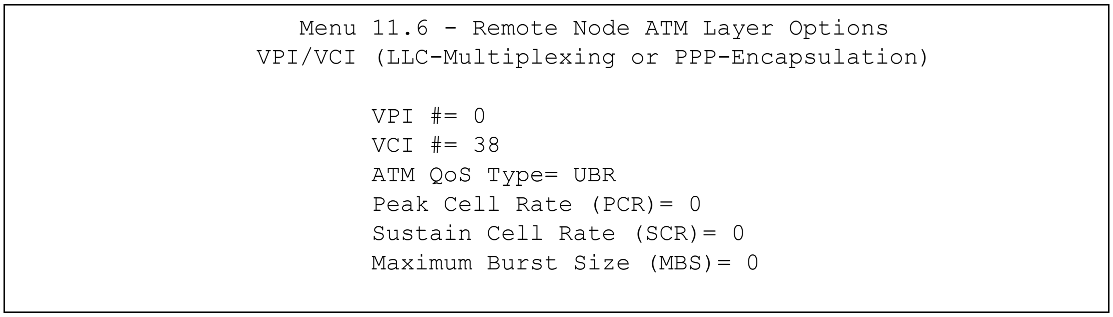
Table 66 Menu 11.5: Remote Node Filter

FIELD	DESCRIPTION
Input Filter Sets	
protocol filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
device filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
Output Filter Sets	
protocol filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
device filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
Call Filter Sets	These fields appear if you selected **PPPoA** or **PPPoE** in **Encapsulation** in menu 11.1.
protocol filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).
device filters	Enter up to four filter sets. If you enter more than one, separate each one with a comma (,).

22.6 Remote Node ATM Layer Options

Move the cursor to the **Edit ATM Options** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open this menu. This menu depends on the multiplexing and encapsulation you select in menu 11.1.

Figure 109 Menu 11.6: Remote Node ATM Layer Options



```
                    Menu 11.6 - Remote Node ATM Layer Options
                 VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)

                         VPI #= 0
                         VCI #= 38
                         ATM QoS Type= UBR
                         Peak Cell Rate (PCR)= 0
                         Sustain Cell Rate (SCR)= 0
                         Maximum Burst Size (MBS)= 0
```

The following table describes the fields in this menu.

Table 67 Menu 11.6: Remote Node ATM Layer Options

FIELD	DESCRIPTION
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.

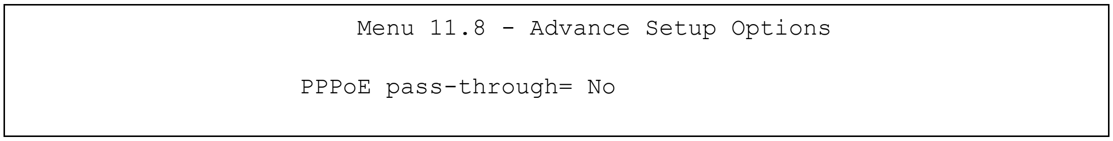
Table 67 Menu 11.6: Remote Node ATM Layer Options (continued)

FIELD	DESCRIPTION
ATM QoS Type	Select **CBR** (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate (PCR)	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate (SCR)	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size (MBS)	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Once you have completed filling in this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration and return to menu 11.1, or press [ESC] at any time to cancel.	

22.7 Advance Setup Options

Move the cursor to the **Edit Advance Options** field in menu 11.1 (only for remote node 1), then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.8 - Advanced Setup Options**.

Figure 110 Menu 11.8: Advance Setup Options



```
                    Menu 11.8 - Advance Setup Options

                PPPoE pass-through= No
```

The following table describes the fields in this menu.

Table 68 Menu 11.8: Advance Setup Options

FIELD	DESCRIPTION
PPPoE pass-through	In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE Passthrough to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for applications where NAT is not appropriate. Disable PPPoE passthrough if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Once you have completed filling in this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration and return to menu 11.1, or press [ESC] at any time to cancel.	

23

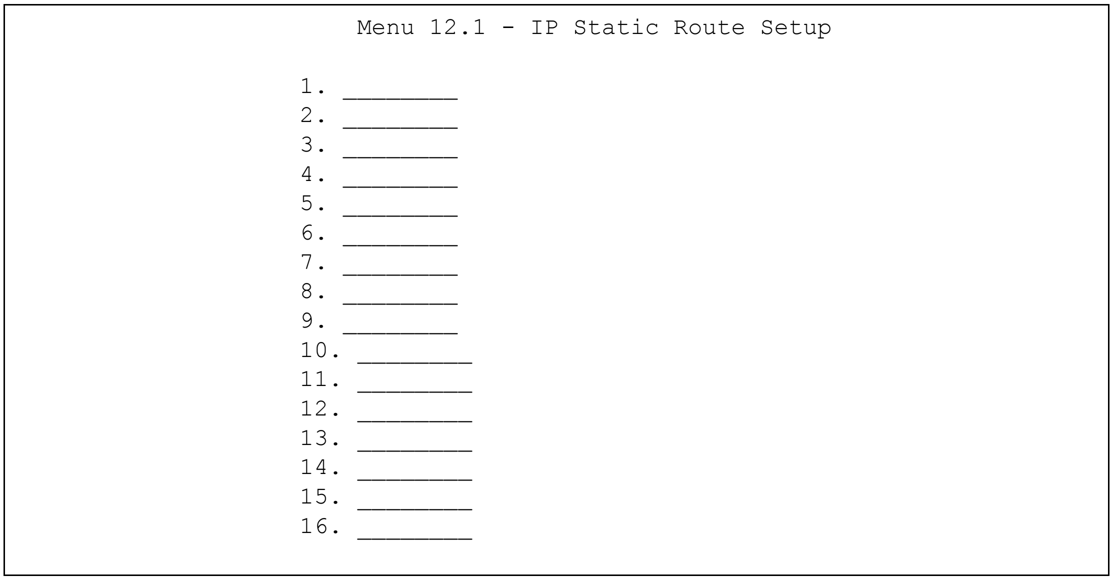
Static Route Setup

Use this menu to configure IP and bridge (MAC) static routes.

23.1 IP Static Route Setup

Enter 1 from the menu 12. Select one of the IP static routes as shown next to configure IP static routes in menu 12.1.

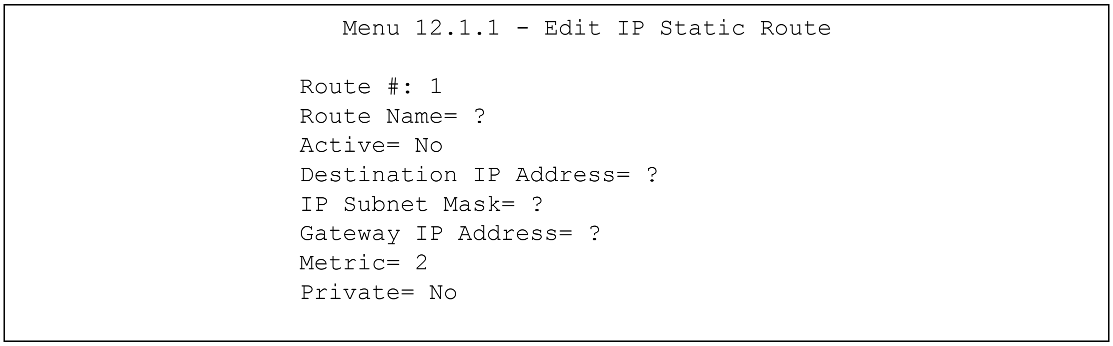
Figure 111 Menu 12.1: IP Static Route Setup



```
                Menu 12.1 - IP Static Route Setup

             1. _________
             2. _________
             3. _________
             4. _________
             5. _________
             6. _________
             7. _________
             8. _________
             9. _________
             10. _________
             11. _________
             12. _________
             13. _________
             14. _________
             15. _________
             16. _________
```

Now, enter the index number of the static route that you want to configure.

Figure 112 Menu 12.1.1: Edit IP Static Route



```
                    Menu 12.1.1 - Edit IP Static Route

                Route #: 1
                Route Name= ?
                Active= No
                Destination IP Address= ?
                IP Subnet Mask= ?
                Gateway IP Address= ?
                Metric= 2
                Private= No
```

The following table describes the fields in this screen.

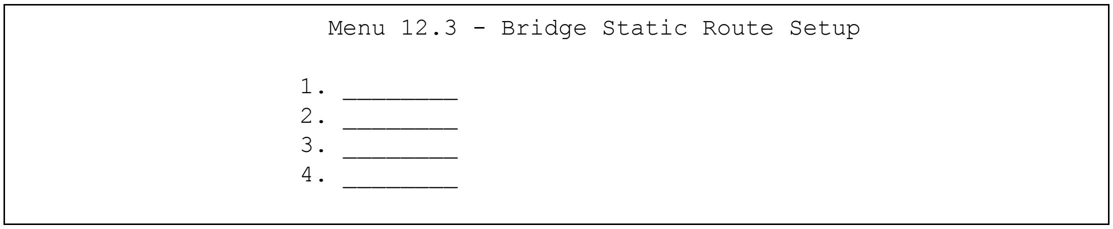
Table 69 Menu 12.1.1: Edit IP Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your ZyXEL Device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyXEL Device; over the WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyXEL Device's routes (see Section 5.2 on page 63). The smaller the number, the higher priority the route has.
Private	This parameter determines if the ZyXEL Device will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
Once you have completed filling in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.	

23.2 Bridge Static Route Setup

Enter 3 from menu 12. Select one of the bridge static routes as shown next to configure IP static routes in menu 12.3.

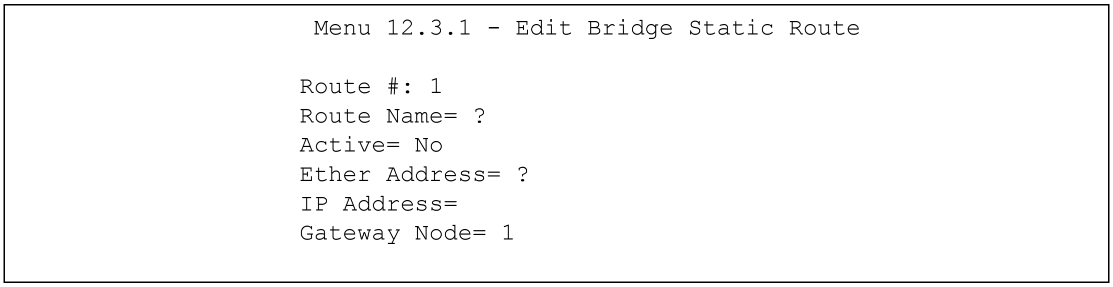
Figure 113 Menu 12.3: Bridge Static Route Setup



```
                      Menu 12.3 - Bridge Static Route Setup

                    1. ________
                    2. ________
                    3. ________
                    4. ________
```

Now, enter the index number of the static route that you want to configure.

Figure 114 Menu 12.3.1: Edit Bridge Static Route



```
                     Menu 12.3.1 - Edit Bridge Static Route

                    Route #: 1
                    Route Name= ?
                    Active= No
                    Ether Address= ?
                    IP Address=
                    Gateway Node= 1
```

The following table describes the fields in this screen.

Table 70 Menu 12.3.1: Edit Bridge Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	This field allows you to activate/deactivate this static route.
Ether Address	This parameter specifies the MAC address of the final destination.
IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your ZyXEL Device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyXEL Device; over the WAN, the gateway must be the IP address of one of the remote nodes.
Gateway Node	Press [SPACE BAR] and then [ENTER] to select the number of the remote node that is the gateway for this static route.
Once you have completed filling in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.	

24

NAT Setup

Use this menu to configure Network Address Translation (NAT) on the ZyXEL Device.

24.1 Using NAT

24.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See Section 24.2.1 on page 201 for a detailed description of the NAT set for SUA. The ZyXEL Device also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

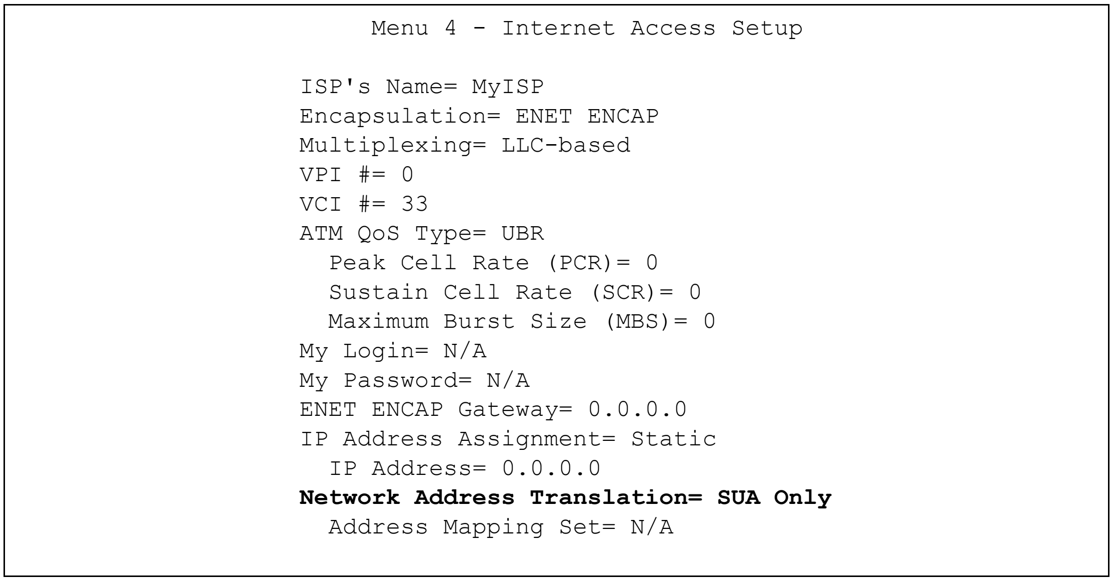
Choose **SUA Only** if you have just one public WAN IP address for your ZyXEL Device.

Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyXEL Device.

24.1.2 Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

Figure 115 Menu 4: Applying NAT for Internet Access

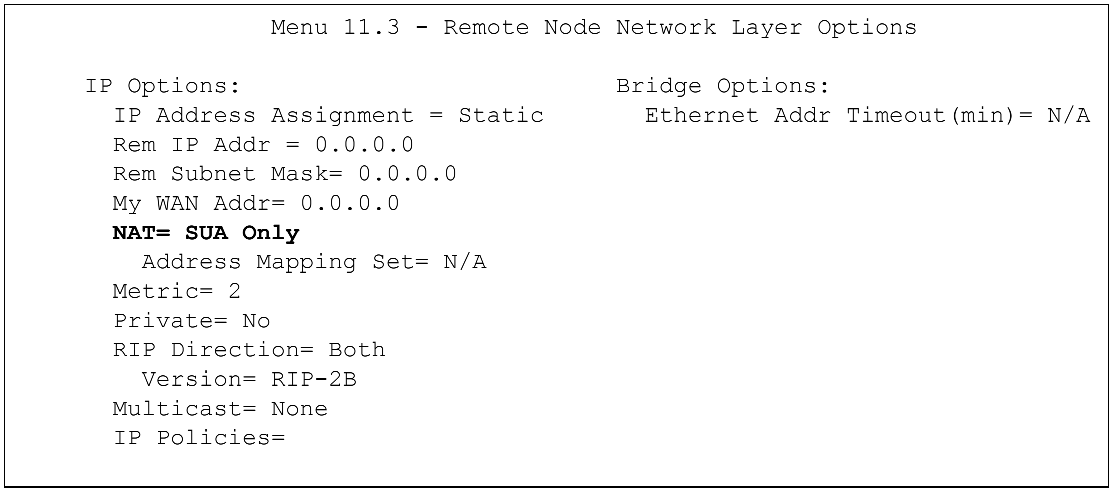


```
                    Menu 4 - Internet Access Setup

               ISP's Name= MyISP
               Encapsulation= ENET ENCAP
               Multiplexing= LLC-based
               VPI #= 0
               VCI #= 33
               ATM QoS Type= UBR
                 Peak Cell Rate (PCR)= 0
                 Sustain Cell Rate (SCR)= 0
                 Maximum Burst Size (MBS)= 0
               My Login= N/A
               My Password= N/A
               ENET ENCAP Gateway= 0.0.0.0
               IP Address Assignment= Static
                 IP Address= 0.0.0.0
               Network Address Translation= SUA Only
                 Address Mapping Set= N/A
```

The following figure shows how you apply NAT to the remote node in menu 11.3.

1. Enter 11 from the main menu.
2. Enter 1 to open **Menu 11.1 - Remote Node Profile**.
3. Move the cursor to the **Edit IP/Bridge** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options**.

Figure 116 Menu 11.3: Applying NAT to the Remote Node



```
             Menu 11.3 - Remote Node Network Layer Options

  IP Options:                          Bridge Options:
    IP Address Assignment = Static       Ethernet Addr Timeout(min)= N/A
    Rem IP Addr = 0.0.0.0
    Rem Subnet Mask= 0.0.0.0
    My WAN Addr= 0.0.0.0
    NAT= SUA Only
      Address Mapping Set= N/A
    Metric= 2
    Private= No
    RIP Direction= Both
      Version= RIP-2B
    Multicast= None
    IP Policies=
```

The following table describes the fields in this menu.

Table 71 Applying NAT in Menus 4 & 11.3

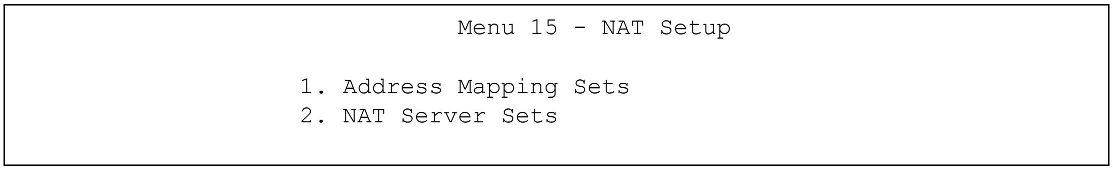
FIELD	DESCRIPTION	OPTIONS
Network Address Translation	When you select this option the SMT will use the specified address mapping set (menu 15.1 - see Section 24.2.1 on page 201 for further discussion). You can configure any of the mapping types described in Chapter 7 on page 93. Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyXEL Device. When you select **Full Feature** you must configure at least one address mapping set.	Full Feature
	NAT is disabled when you select this option.	None
	When you select this option the SMT will use Address Mapping Set 255 (menu 15.1 - see Section 24.2.1 on page 201). Choose **SUA Only** if you have just one public WAN IP address for your ZyXEL Device.	SUA Only

24.2 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN and the DMZ. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or menu 11.3, the SMT will use the address mapping set that you specify. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

A server set is a list of LAN servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the section on port forwarding in Section 7.4 on page 97 for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

Figure 117 Menu 15: NAT Setup

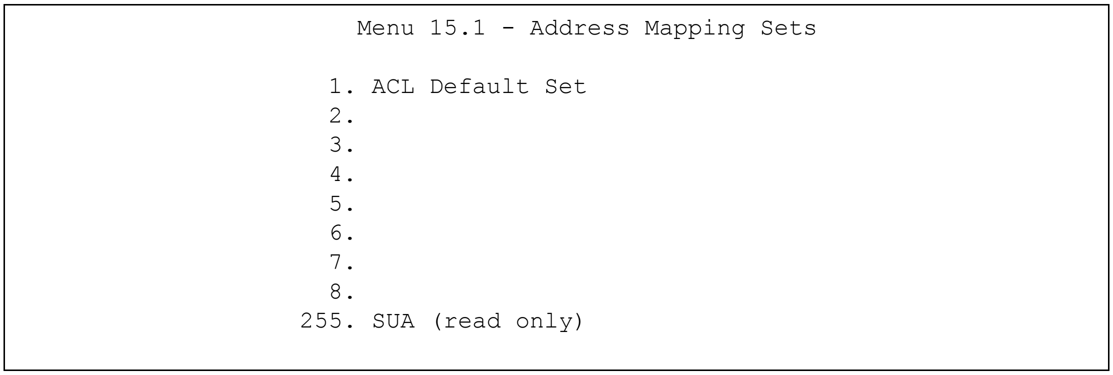


```
                          Menu 15 - NAT Setup

                 1. Address Mapping Sets
                 2. NAT Server Sets
```

24.2.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1.1 - Address Mapping Sets**.

Figure 118 Menu 15.1: Address Mapping Sets



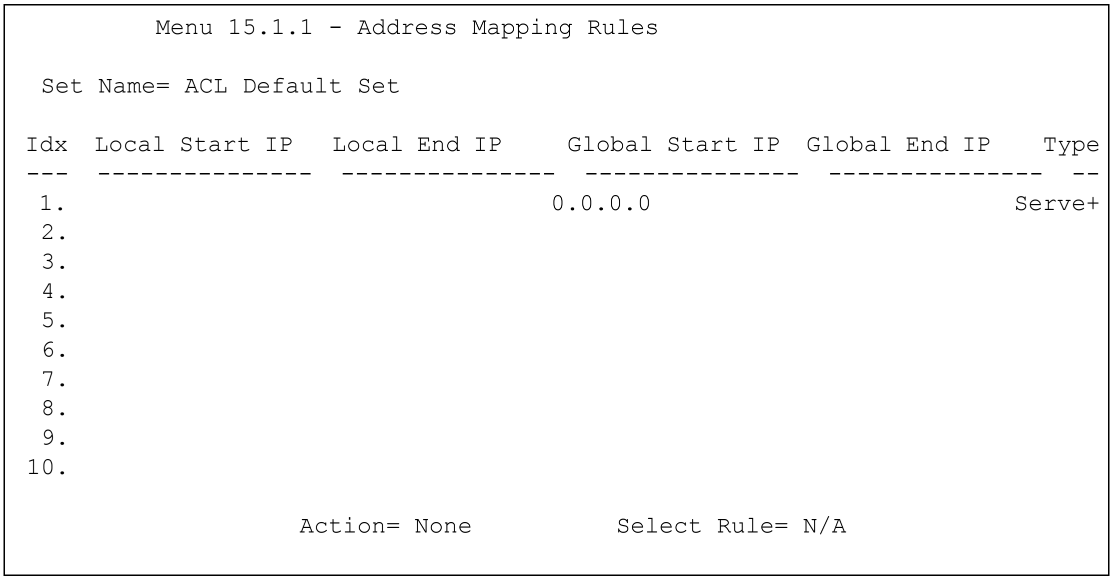
```
                        Menu 15.1 - Address Mapping Sets

                      1. ACL Default Set
                      2.
                      3.
                      4.
                      5.
                      6.
                      7.
                      8.
                    255. SUA (read only)
```

Select the address mapping set you want to modify. The fields in address 255 are used for SUA and are read-only.

24.2.1.1 User-Defined Address Mapping Sets

The entire set will be deleted if you leave the **Set Name** field blank and press [ENTER] at the bottom of the screen.

Figure 119 Menu 15.1.1: Address Mapping Rules



```
          Menu 15.1.1 - Address Mapping Rules

  Set Name= ACL Default Set

 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
 ---  ---------------  ---------------  ---------------  ---------------  --
  1.                                  0.0.0.0                         Serve+
  2.
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.

                    Action= None          Select Rule= N/A
```

The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

Table 72 Menu 15.1.1: Address Mapping Rules

FIELD	DESCRIPTION
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.
Idx	This is the index or rule number.
Local Start IP	**Local Start IP** is the starting local IP address (ILA).
Local End IP	**Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the start IP is 0.0.0.0 and the end IP is 255.255.255.255.
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.
Global End IP	This is the ending global IP address (IGA).
Type	These are the mapping types discussed above. **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.
Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.	

Ordering your rules is important because the ZyXEL Device applies the rules in the order that you specify. When a rule matches the current packet, the ZyXEL Device takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

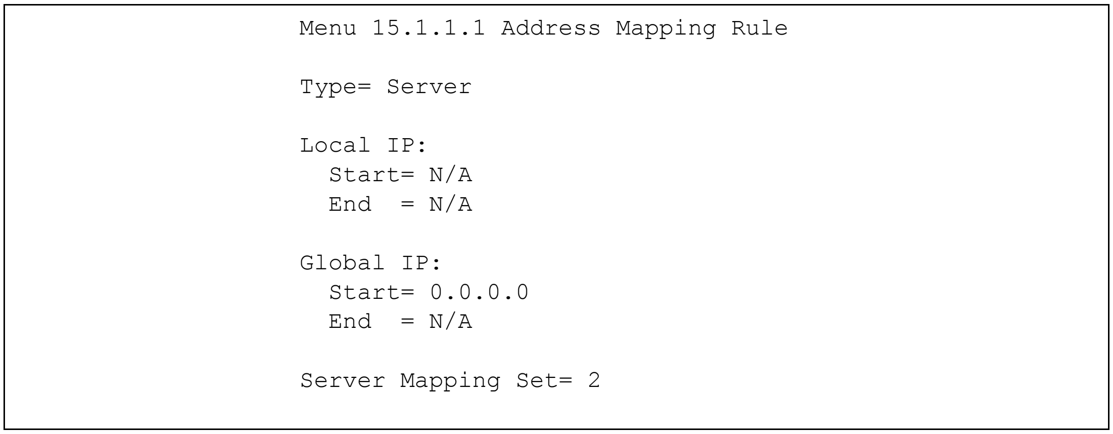
Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

An IP End address must be numerically greater than its corresponding IP Start address.

Figure 120 Menu 15.1.1.1: Address Mapping Rule



```
Menu 15.1.1.1 Address Mapping Rule

Type= Server

Local IP:
  Start= N/A
  End  = N/A

Global IP:
  Start= 0.0.0.0
  End  = N/A

Server Mapping Set= 2
```

The following table describes the fields in this menu.

Table 73 Menu 15.1.1.1: Address Mapping Rule

FIELD	DESCRIPTION
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in Chapter 7 on page 93. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See Section 24.4.3 on page 208 for an example.
Local IP	These fields are enabled depending on the **Type**.
Start	Enter the starting local IP address (ILA).
End	Enter the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.
Global IP	These fields are enabled depending on the **Type**.
Start	Enter the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**.
End	Enter the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.
Server Mapping Set	This field is available only when you select **Server** in the **Type** field. Select which server mapping set to use for this rule.
Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.	

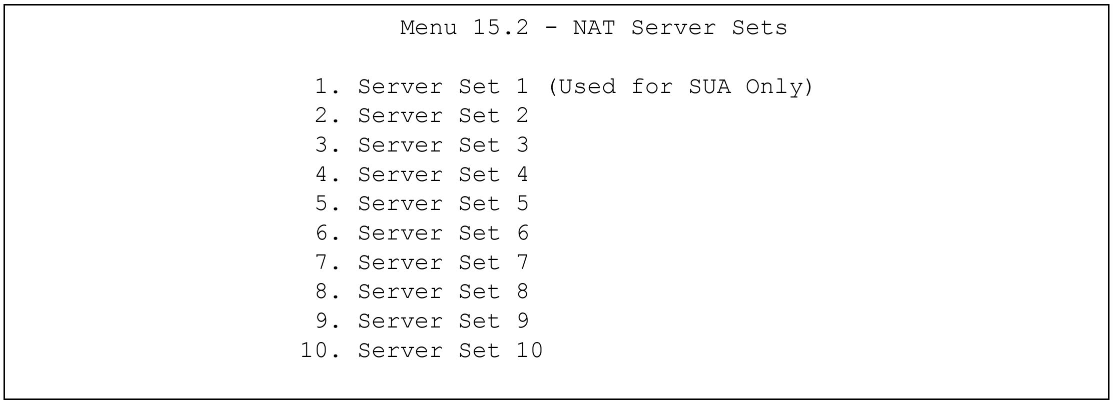
24.3 Configuring a Server behind NAT

If you do not assign a **Default Server** IP address, the ZyXEL Device discards all packets received for ports that are not specified here or in the remote management setup.

Follow these steps to configure a server behind NAT:

1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup.**
2. Enter 2 to open menu 15.2 (and configure the address mapping rules for the WAN port on a ZyXEL Device with a single WAN port).

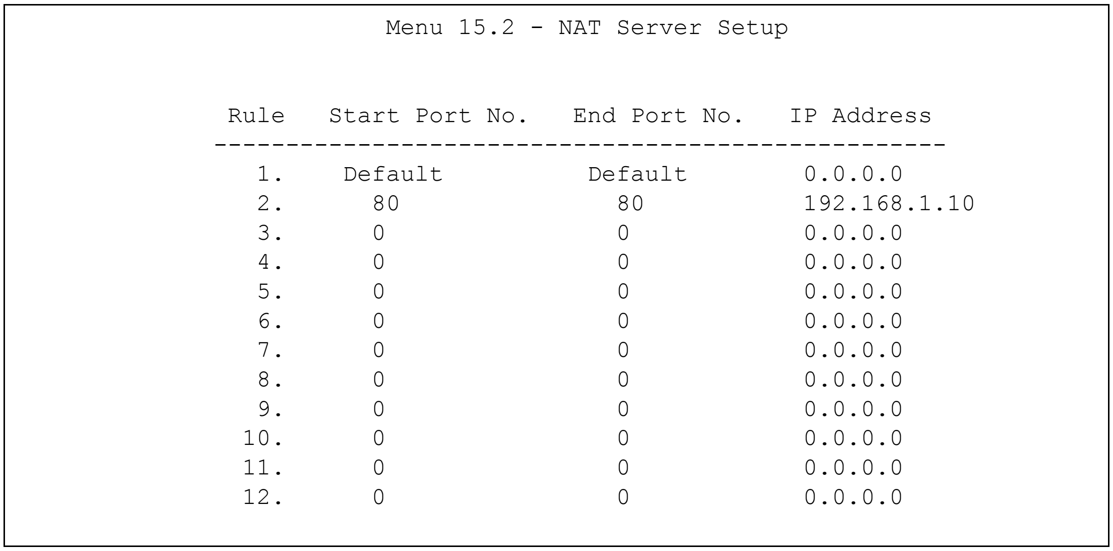
Figure 121 Menu 15.2: NAT Server Sets



```
                     Menu 15.2 - NAT Server Sets

               1. Server Set 1 (Used for SUA Only)
               2. Server Set 2
               3. Server Set 3
               4. Server Set 4
               5. Server Set 5
               6. Server Set 6
               7. Server Set 7
               8. Server Set 8
               9. Server Set 9
              10. Server Set 10
```

3. Enter 1 to configure the server set used by SUA, or enter the number of the server set you want to modify for full-feature NAT. In **Menu 15.2 - NAT Server Setup**, configure the port forwarding rules.

Figure 122 Menu 15.2: NAT Server Setup



```
                    Menu 15.2 - NAT Server Setup


          Rule   Start Port No.   End Port No.   IP Address
         ---------------------------------------------------
            1.    Default          Default        0.0.0.0
            2.      80               80           192.168.1.10
            3.      0                0            0.0.0.0
            4.      0                0            0.0.0.0
            5.      0                0            0.0.0.0
            6.      0                0            0.0.0.0
            7.      0                0            0.0.0.0
            8.      0                0            0.0.0.0
            9.      0                0            0.0.0.0
           10.      0                0            0.0.0.0
           11.      0                0            0.0.0.0
           12.      0                0            0.0.0.0
```

The first entry is for the **Default Server**. The following table describes the labels in this menu.

Table 74 Menu 15.2: NAT Server Setup

FIELD	DESCRIPTION
Rule	This field is a sequential value, and it is not associated with a specific rule. The sequence is important, however. The ZyXEL Device checks each active rule in order, and it only follows the first one that applies.
Start Port	This field displays the beginning of the range of port numbers forwarded by this rule.
End Port	This field displays the end of the range of port numbers forwarded by this rule. If it is the same as the **Start Port**, only one port number is forwarded.
IP Address	This field displays the IP address of the server to which packet for the selected port(s) are forwarded.

24.4 General NAT Examples

The following are some examples of NAT configuration.

24.4.1 Internet Access Only

In the following Internet access example, you only need one rule where all your ILAs (Inside Local addresses) map to one dynamic IGA (Inside Global Address) assigned by your ISP.

Figure 123 NAT Example 1

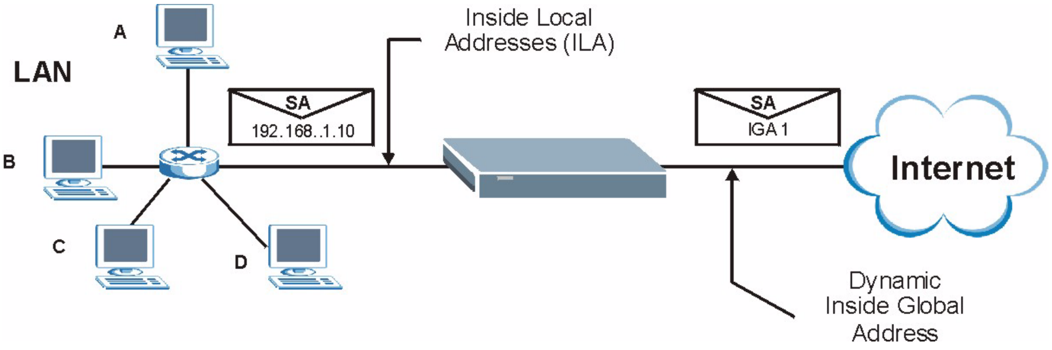
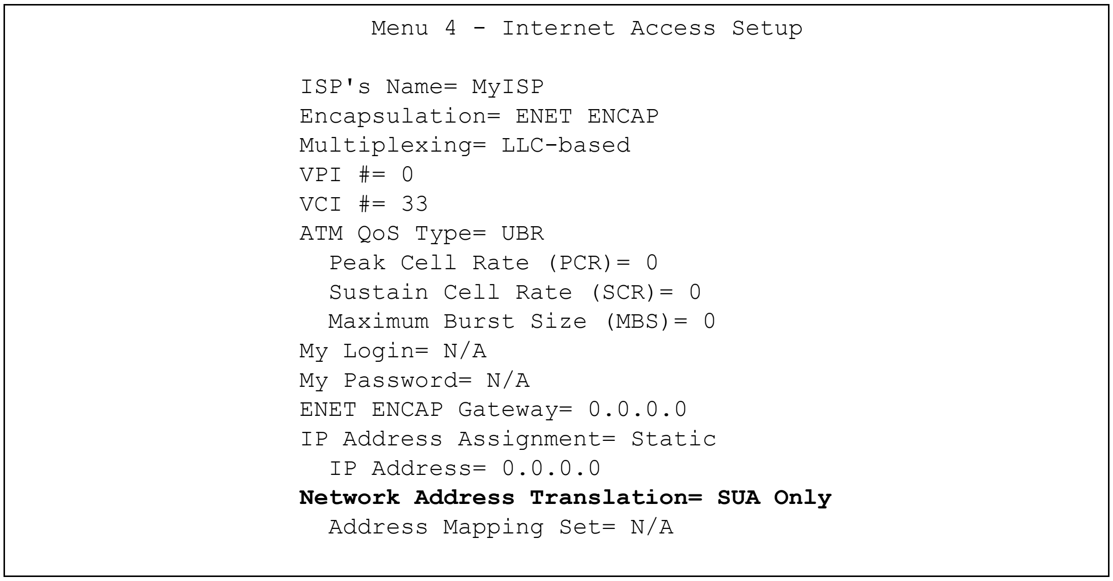


Figure 124 Menu 4: Internet Access & NAT Example

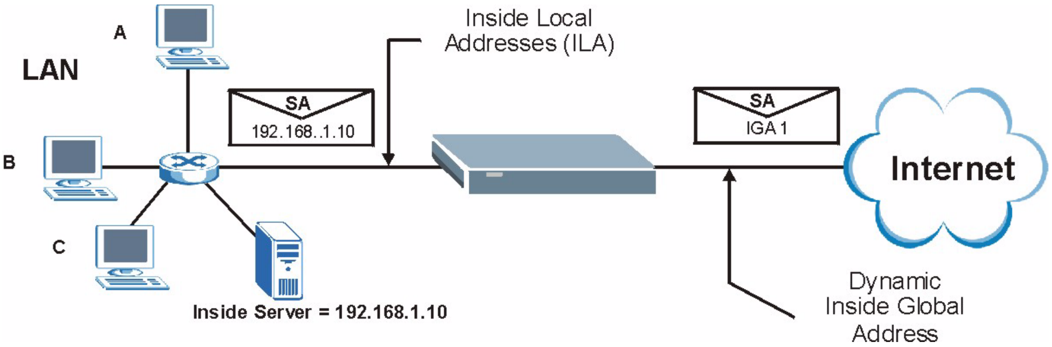


```
                    Menu 4 - Internet Access Setup

               ISP's Name= MyISP
               Encapsulation= ENET ENCAP
               Multiplexing= LLC-based
               VPI #= 0
               VCI #= 33
               ATM QoS Type= UBR
                 Peak Cell Rate (PCR)= 0
                 Sustain Cell Rate (SCR)= 0
                 Maximum Burst Size (MBS)= 0
               My Login= N/A
               My Password= N/A
               ENET ENCAP Gateway= 0.0.0.0
               IP Address Assignment= Static
                 IP Address= 0.0.0.0
               Network Address Translation= SUA Only
                 Address Mapping Set= N/A
```

From menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in Section 24.4 on page 206. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

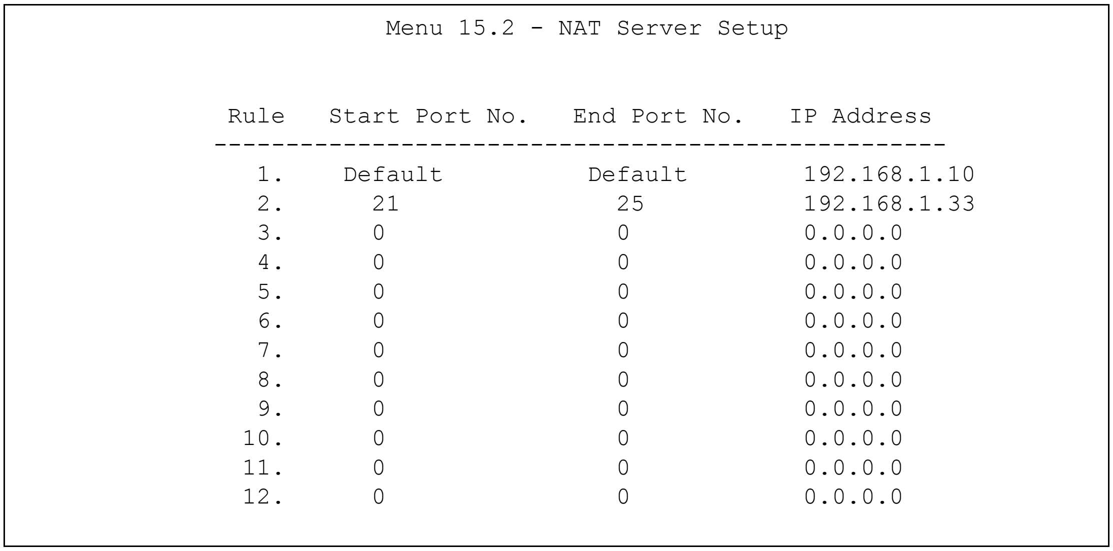
24.4.2 Example 2: Internet Access with a Default Server

Figure 125 NAT Example 2



In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2.1 to specify the **Default Server** behind the NAT as shown in the next figure.

Figure 126 Menu 15.2: Specifying an Inside Server



```
                        Menu 15.2 - NAT Server Setup


           Rule   Start Port No.   End Port No.   IP Address
          ---------------------------------------------------
             1.     Default          Default        192.168.1.10
             2.       21               25           192.168.1.33
             3.       0                0            0.0.0.0
             4.       0                0            0.0.0.0
             5.       0                0            0.0.0.0
             6.       0                0            0.0.0.0
             7.       0                0            0.0.0.0
             8.       0                0            0.0.0.0
             9.       0                0            0.0.0.0
            10.       0                0            0.0.0.0
            11.       0                0            0.0.0.0
            12.       0                0            0.0.0.0
```

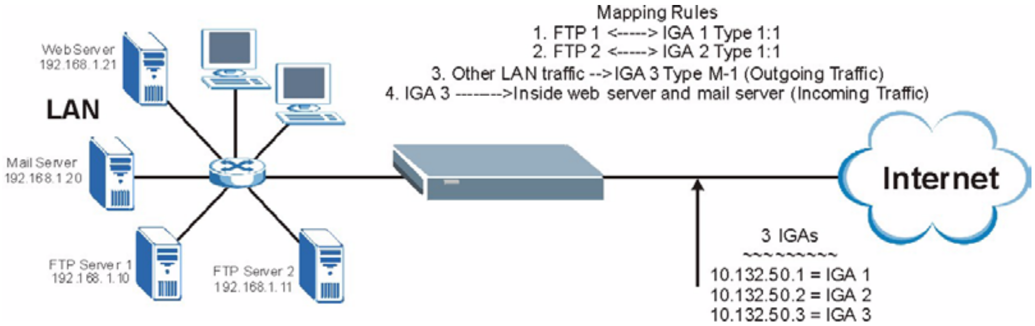
24.4.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two uni-directional as follows.

1. Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
2. Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
3. Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).
4. You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

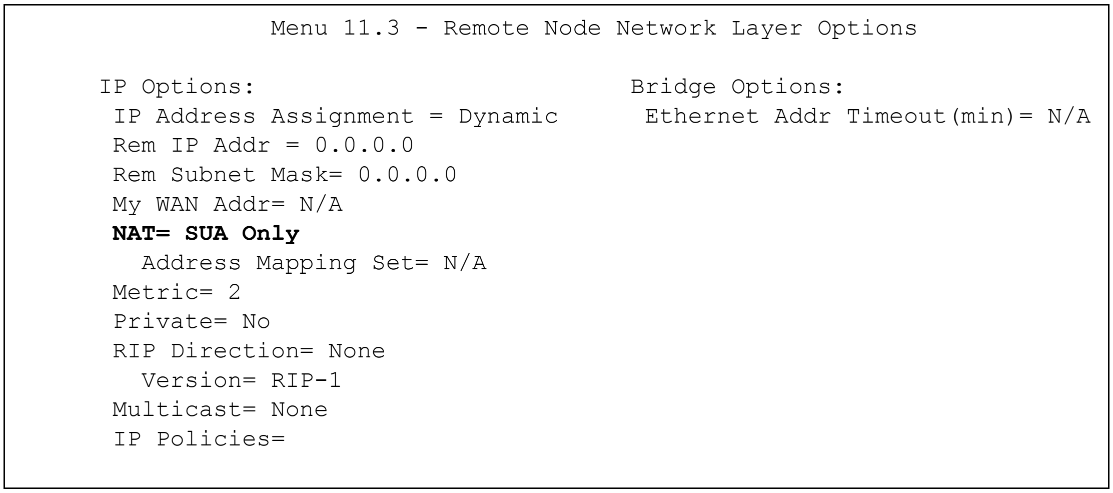
The example situation looks somewhat like this:

Figure 127 NAT Example 3


Mapping Rules
1. FTP 1 <-----> IGA 1 Type 1:1
2. FTP 2 <-----> IGA 2 Type 1:1
3. Other LAN traffic -->IGA 3 Type M-1 (Outgoing Traffic)
4. IGA 3 -------->Inside web server and mail server (Incoming Traffic)
WebServer
192.168.1.21
LAN
Mail Server
192.168.1.20
FTP Server 1
192.168.1.10
FTP Server 2
192.168.1.11
Internet
3 IGAs
10.132.50.1 = IGA 1
10.132.50.2 = IGA 2
10.132.50.3 = IGA 3

1. In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in Figure 128 on page 209.
2. Then enter 15 from the main menu.
3. Enter 1 to configure the Address Mapping Sets.
4. Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
5. Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See Figure 129 on page 209*)*.
6. Repeat the previous step for rules 2 to 4 as outlined above.
7. When finished, menu 15.1.1 should look like as shown in Figure 130 on page 210.

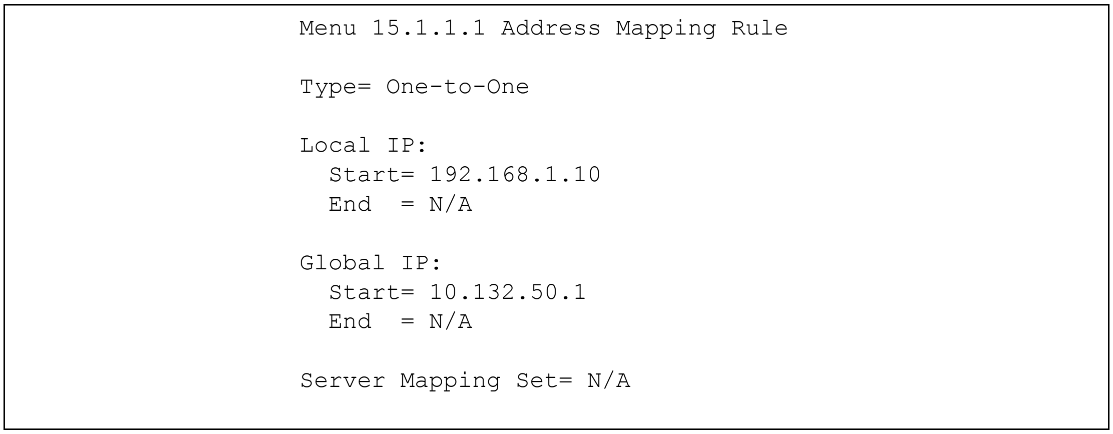
Figure 128 Example 3: Menu 11.3



```
                  Menu 11.3 - Remote Node Network Layer Options

      IP Options:                                 Bridge Options:
       IP Address Assignment = Dynamic             Ethernet Addr Timeout(min)= N/A
       Rem IP Addr = 0.0.0.0
       Rem Subnet Mask= 0.0.0.0
       My WAN Addr= N/A
       NAT= SUA Only
         Address Mapping Set= N/A
       Metric= 2
       Private= No
       RIP Direction= None
         Version= RIP-1
       Multicast= None
       IP Policies=
```

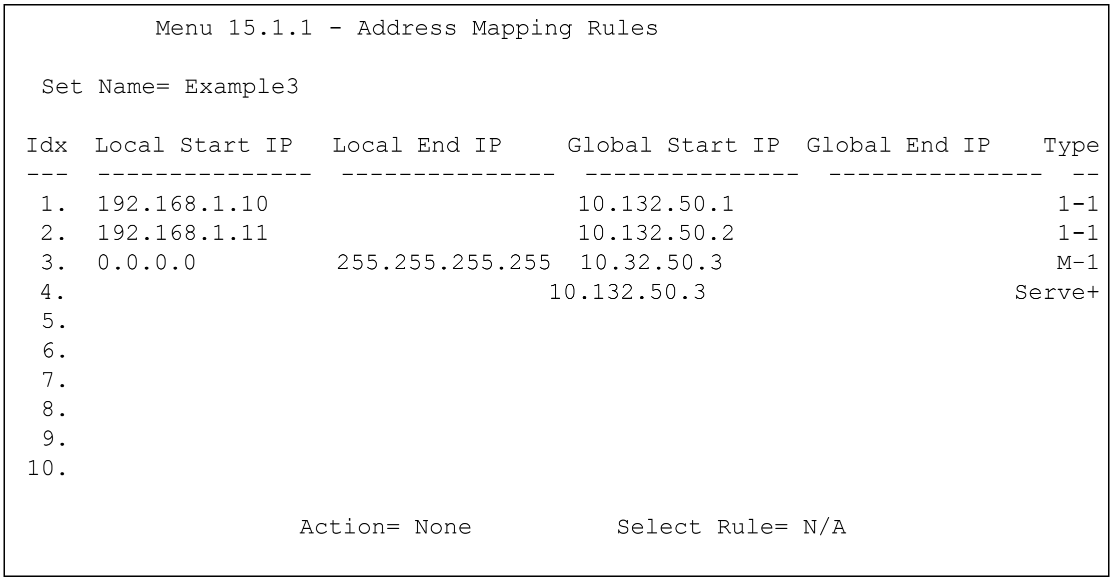
The following figure shows how to configure the first rule.

Figure 129 Example 3: Menu 15.1.1.1



```
                    Menu 15.1.1.1 Address Mapping Rule

                    Type= One-to-One

                    Local IP:
                      Start= 192.168.1.10
                      End   = N/A

                    Global IP:
                      Start= 10.132.50.1
                      End   = N/A

                    Server Mapping Set= N/A
```

Figure 130 Example 3: Final Menu 15.1.1

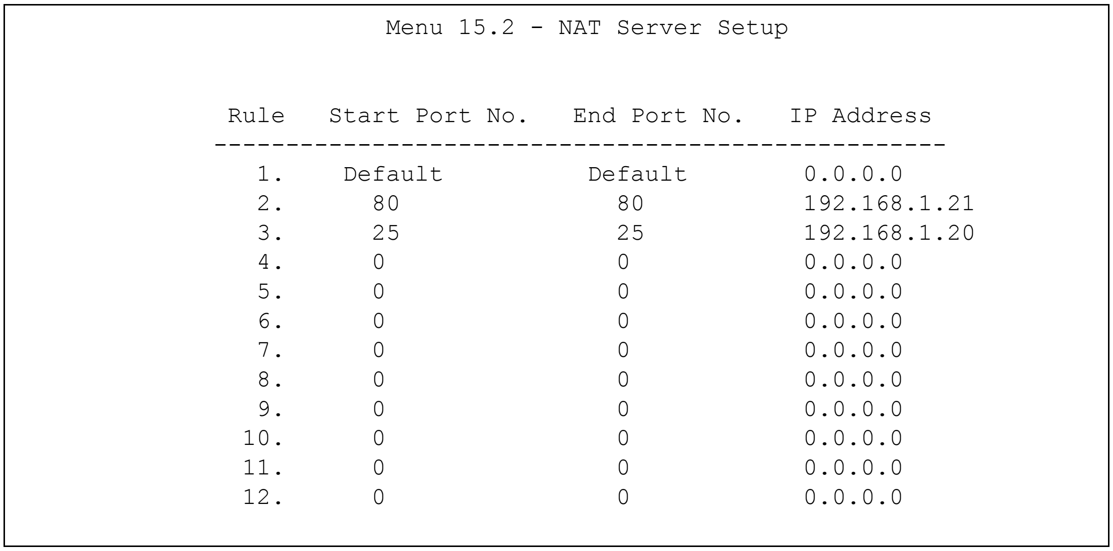


```
          Menu 15.1.1 - Address Mapping Rules

  Set Name= Example3

 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
 ---  ---------------  ---------------  ---------------  ---------------  --
  1.  192.168.1.10                       10.132.50.1                      1-1
  2.  192.168.1.11                       10.132.50.2                      1-1
  3.  0.0.0.0         255.255.255.255   10.32.50.3                        M-1
  4.                                   10.132.50.3                     Serve+
  5.
  6.
  7.
  8.
  9.
 10.

                    Action= None          Select Rule= N/A
```

Now configure the IGA3 to map to our web server and mail server on the LAN.

1. Enter 15 from the main menu.
2. Enter 2 to go to menu 15.2.
3. (Enter 1 or 2 from menu 15.2 on a ZyXEL Device with multiple WAN ports) configure the menu as shown in Figure 131 on page 210.

Figure 131 Example 3: Menu 15.2

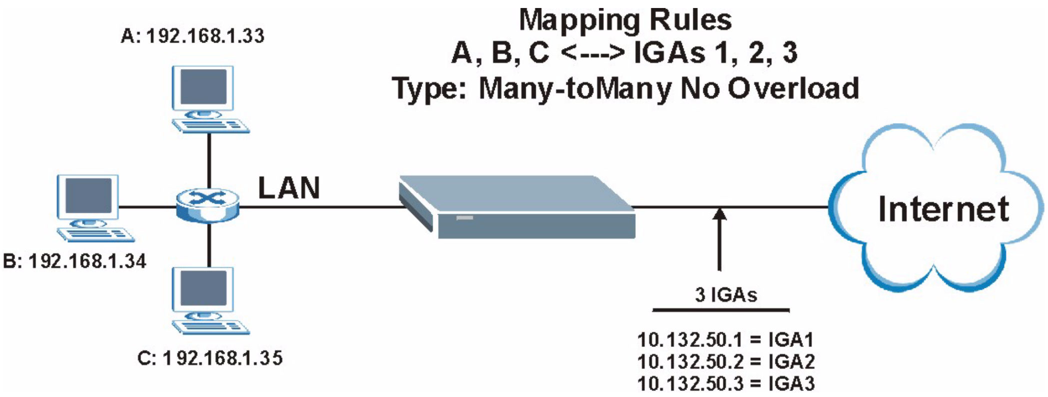


```
                         Menu 15.2 - NAT Server Setup


               Rule   Start Port No.   End Port No.   IP Address
              ---------------------------------------------------
                 1.    Default          Default         0.0.0.0
                 2.      80               80            192.168.1.21
                 3.      25               25            192.168.1.20
                 4.     0                0              0.0.0.0
                 5.     0                0              0.0.0.0
                 6.     0                0              0.0.0.0
                 7.     0                0              0.0.0.0
                 8.     0                0              0.0.0.0
                 9.     0                0              0.0.0.0
                10.     0                0              0.0.0.0
                11.     0                0              0.0.0.0
                12.     0                0              0.0.0.0
```

24.4.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-One-to-One** mapping as port numbers do *not* change for **Many-One-to-One** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

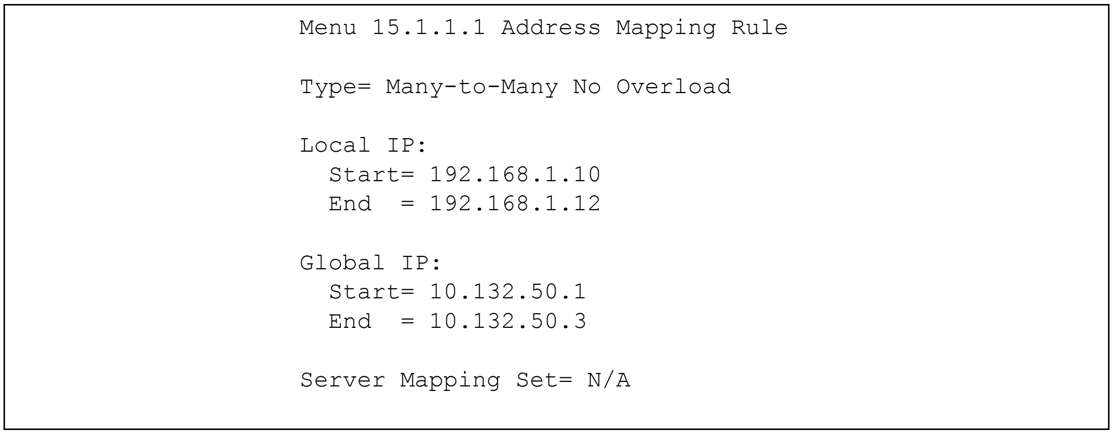
Figure 132 NAT Example 4



Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won’t work through NAT even when using **One-to-One** and **Many-One-to-One** mapping types.

Follow the steps outlined in example 3 above to configure these two menus as follows.

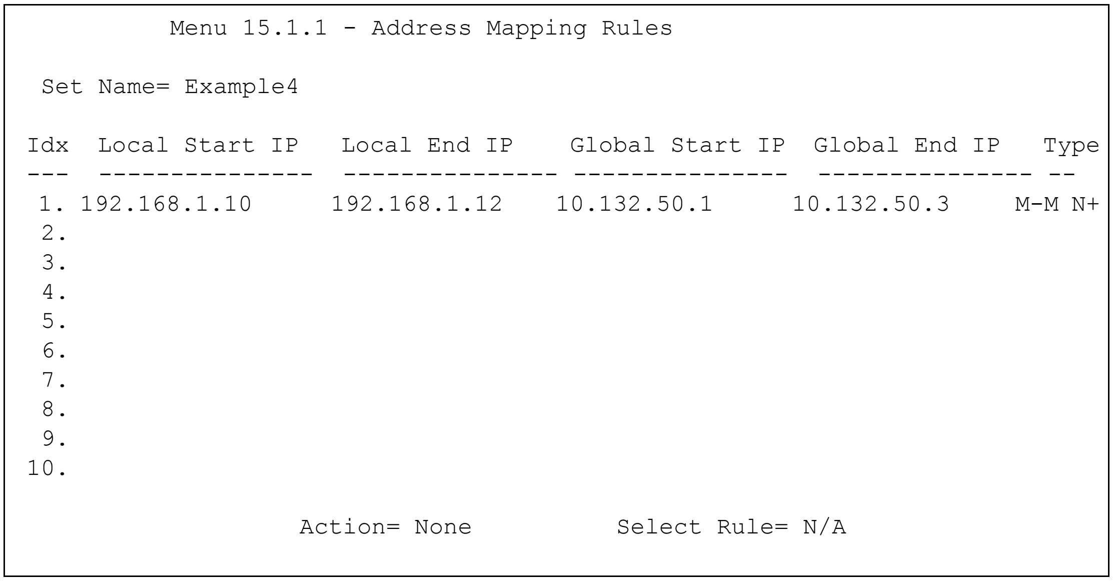
Figure 133 Example 4: Menu 15.1.1.1: Address Mapping Rule



```
Menu 15.1.1.1 Address Mapping Rule

Type= Many-to-Many No Overload

Local IP:
  Start= 192.168.1.10
  End  = 192.168.1.12

Global IP:
  Start= 10.132.50.1
  End  = 10.132.50.3

Server Mapping Set= N/A
```

After you’ve configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

Figure 134   Example 4: Menu 15.1.1: Address Mapping Rules



```
          Menu 15.1.1 - Address Mapping Rules

 Set Name= Example4

Idx  Local Start IP   Local End IP    Global Start IP  Global End IP   Type
---  ---------------  --------------- ---------------  --------------- --
 1. 192.168.1.10     192.168.1.12    10.132.50.1      10.132.50.3     M-M N+
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                  Action= None          Select Rule= N/A
```

25

Filter Configuration

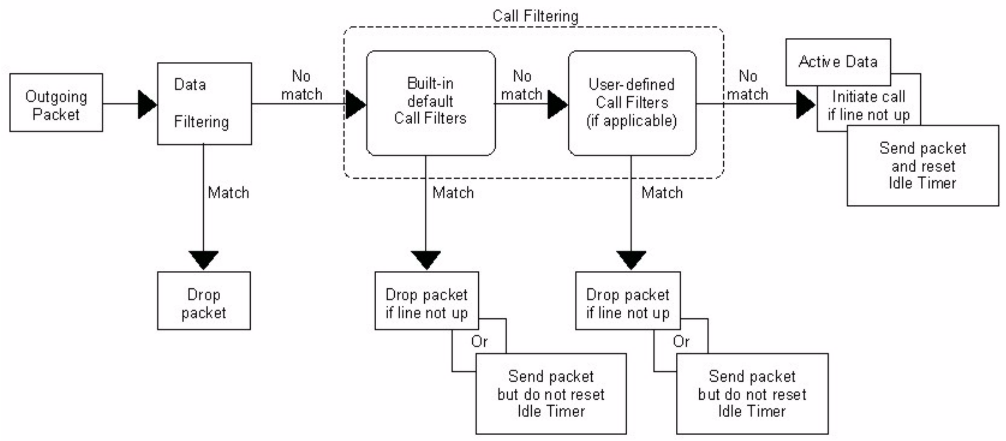
This chapter shows you how to create and apply filters.

25.1 Introduction to Filters

Your ZyXEL Device uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the LAN side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using PPPoE encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

Figure 135 Outgoing Packet Filtering Process



Call Filtering
Outgoing Packet
Data Filtering
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not reset Idle Timer
Drop packet if line not up
Or
Send packet but do not reset Idle Timer

For incoming packets, your ZyXEL Device applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

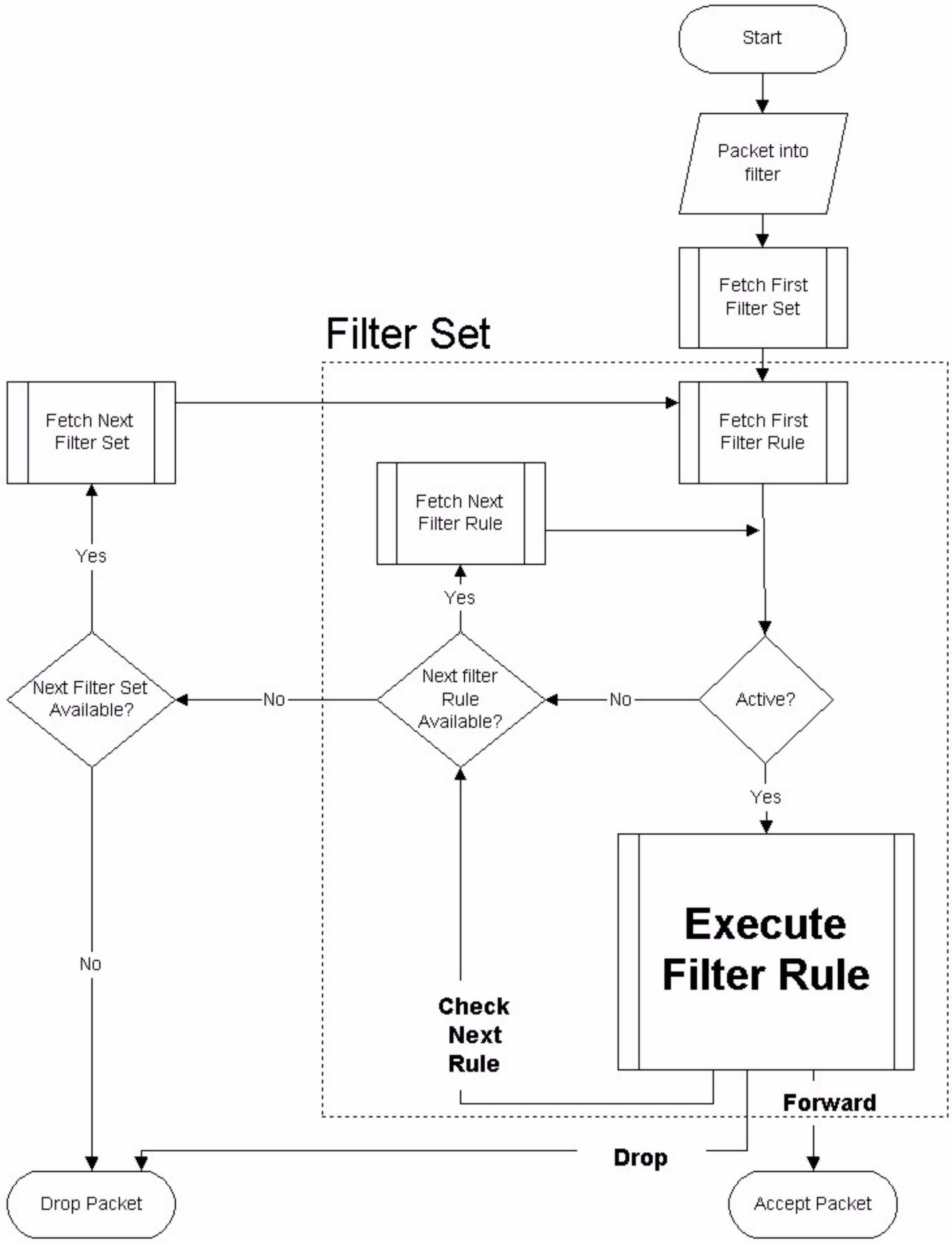
25.1.1 The Filter Structure of the ZyXEL Device

A filter set consists of one or more filter rules. Usually, you would group related rules, for example all the rules for NetBIOS, into a single set and give it a descriptive name. The ZyXEL Device allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming telnet sessions. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule. See also Figure 140 on page 220 for the logic flow when executing an IP filter.

Figure 136 Filter Rule Process



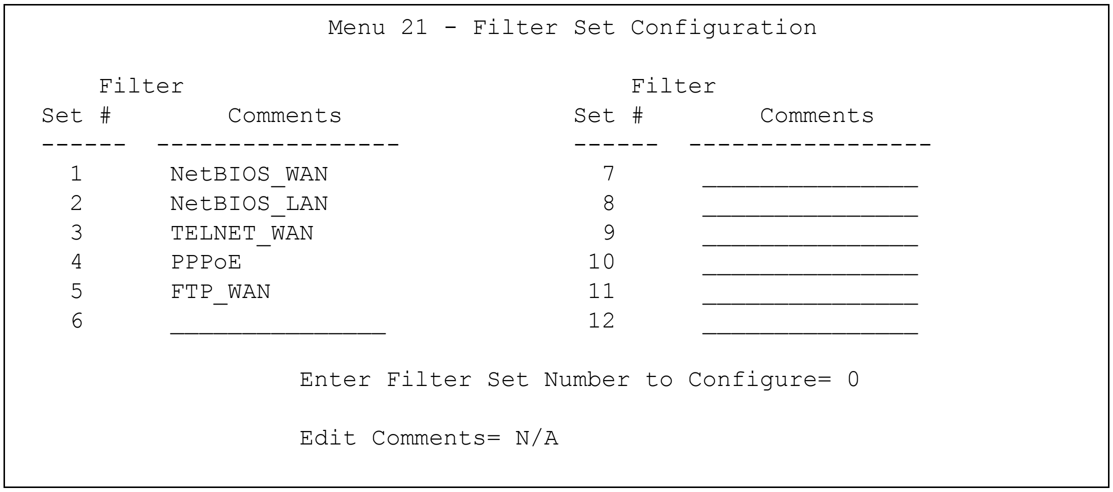
You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

25.2 Configuring a Filter Set

The ZyXEL Device includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

1 Enter 21 in the main menu to open menu 21.

Figure 137 Menu 21: Filter Set Configuration



```
                    Menu 21 - Filter Set Configuration

    Filter                                Filter
 Set #       Comments                  Set #       Comments
 ------  -----------------             ------  -----------------
   1      NetBIOS_WAN                    7      _______________
   2      NetBIOS_LAN                    8      _______________
   3      TELNET_WAN                     9      _______________
   4      PPPoE                         10      _______________
   5      FTP_WAN                       11      _______________
   6      _______________               12      _______________

                  Enter Filter Set Number to Configure= 0

                  Edit Comments= N/A
```

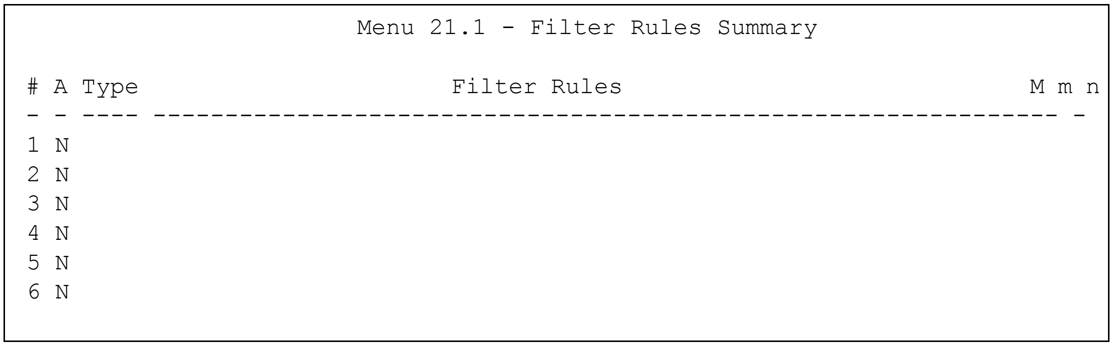
2 Select the filter set you wish to configure (1-12) and press [ENTER].

3 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

4 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.x - Filter Rules Summary**.

This screen shows the summary of the existing rules in the filter set.

Figure 138 Menu 21.1: Filter Rules Summary



```
                       Menu 21.1 - Filter Rules Summary

# A Type                     Filter Rules                            M m n
- - ---- -------------------------------------------------------------- -
1 N
2 N
3 N
4 N
5 N
6 N
```

The following table describes the labels in this screen.

Table 75 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	This is an index number.
A	Active: “Y” means the rule is active. “N” means the rule is inactive.
Type	The type of filter rule: “GEN” for Generic, “IP” for TCP/IP.
Filter Rules	These parameters are displayed here.

Table 75 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
M	More. “Y” means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. “N” means there are no more rules to check. You can specify an action to be taken, in other words forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N“ means to check the next rule.
n	Action Not Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N” means to check the next rule.

The following tables contain a brief description of the abbreviations used in the previous menus. The protocol dependent filter rules abbreviation are listed as follows:

Table 76 Rule Abbreviations Used

ABBREVIATION	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number
GEN	
Off	Offset
Len	Length

Refer to the next section for information on configuring the filter rules.

25.2.1 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.x - Filter Rules Summary** and press [ENTER] to open menu 21.x.x for the rule.

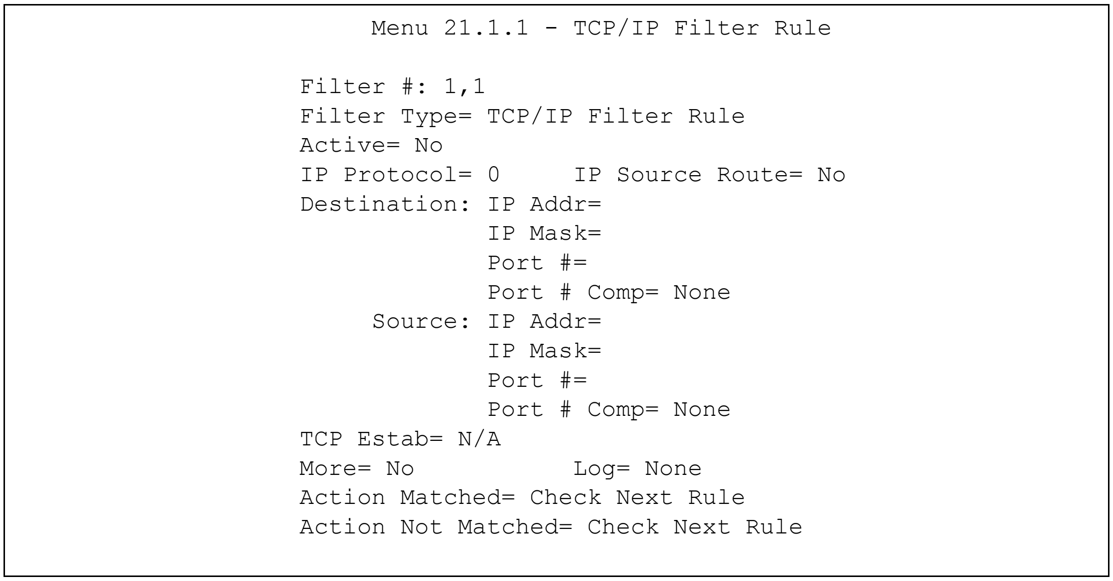
To speed up filtering, all rules in a filter set must be of the same class, that is, protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the ZyXEL Device will warn you and will not allow you to save.

25.2.2 Configuring a TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.x.x - TCP/IP Filter Rule.** Menu 122.1.1 is shown next as an example.

Figure 139 Menu 21.1.1: TCP/IP Filter Rule



```
                         Menu 21.1.1 - TCP/IP Filter Rule

                    Filter #: 1,1
                    Filter Type= TCP/IP Filter Rule
                    Active= No
                    IP Protocol= 0     IP Source Route= No
                    Destination: IP Addr=
                                 IP Mask=
                                 Port #=
                                 Port # Comp= None
                         Source: IP Addr=
                                 IP Mask=
                                 Port #=
                                 Port # Comp= None
                    TCP Estab= N/A
                    More= No           Log= None
                    Action Matched= Check Next Rule
                    Action Not Matched= Check Next Rule
```

The following table describes how to configure your TCP/IP filter rule.

Table 77 Menu 21.1.1: TCP/IP Filter Rule

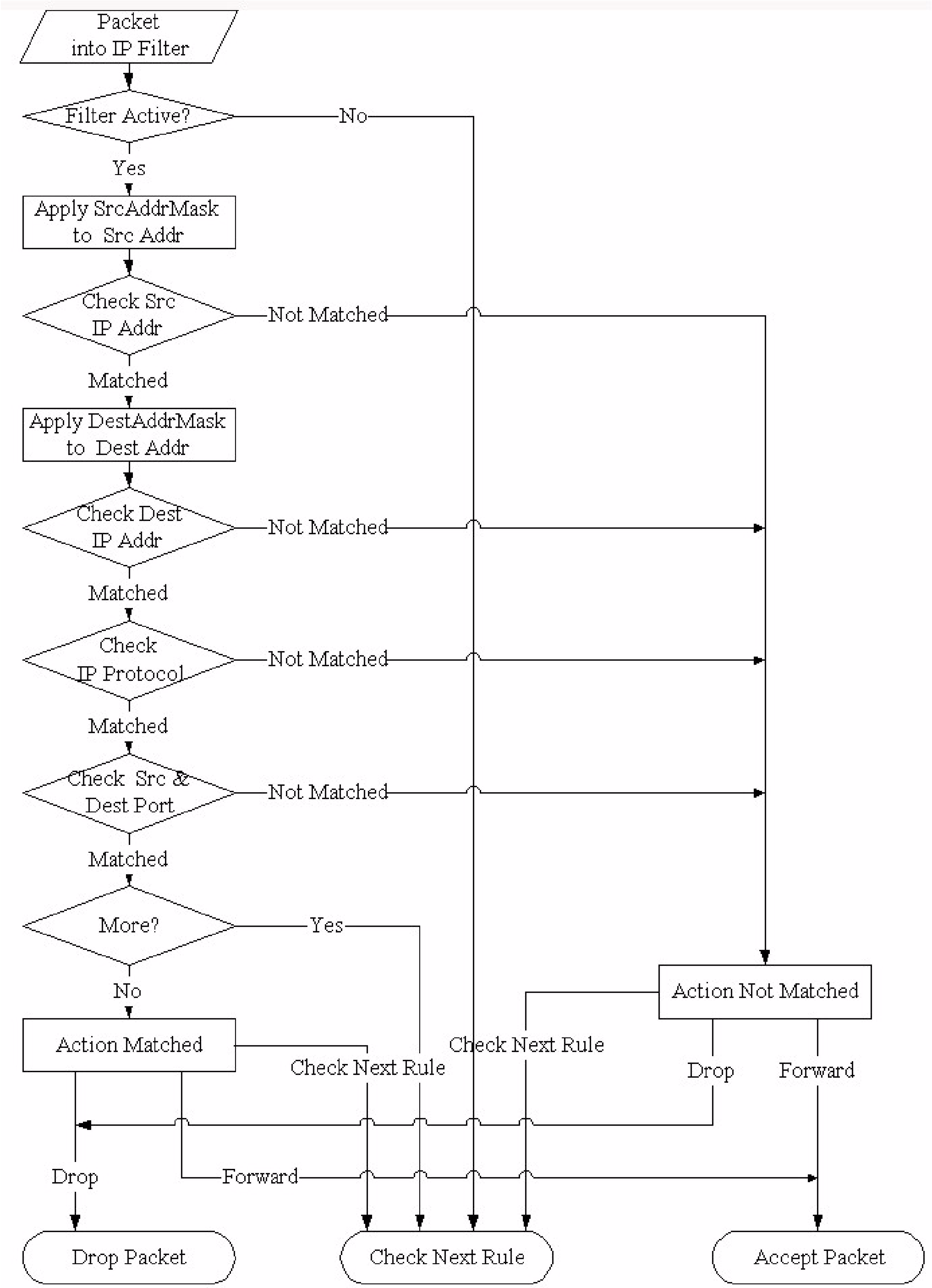
FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the filter rule or **No** to deactivate it.
IP Protocol	Protocol refers to the upper layer protocol, for example TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol.
IP Source Route	Press [SPACE BAR] and then [ENTER] to select **Yes** to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route.
Destination	
IP Addr	Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
IP Mask	Enter the IP mask to apply to the **Destination: IP Addr**.
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given **in Destination: Port #**. Options are **None**, **Equal**, **Not Equal**, **Less** and **Greater**.
Source	
IP Addr	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
IP Mask	Enter the IP mask to apply to the **Source: IP Addr**.
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.

Table 77 Menu 21.1.1: TCP/IP Filter Rule

FIELD	DESCRIPTION
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in **Source: Port #**. Options are **None**, **Equal**, **Not Equal**, **Less** and **Greater**.
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select **Yes**, to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if **No**, it is ignored.
More	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. If **Yes**, a matching packet is passed to the next filter rule before an action is taken; if **No**, the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.
Log	Press [SPACE BAR] and then [ENTER] to select a logging option from the following: **None** – No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.
Action Matched	Press [SPACE BAR] and then [ENTER] to select the action for a matching packet. Options are **Check Next Rule**, **Forward** and **Drop**.
Action Not Matched	Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule. Options are **Check Next Rule**, **Forward** and **Drop**.
When you have **Menu 21.1.1 - TCP/IP Filter Rule** configured, press [ENTER] at the message “Press ENTER to Confirm” to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1 - Filter Rules Summary**.	

The following figure illustrates the logic flow of an IP filter.

Figure 140 Executing an IP Filter



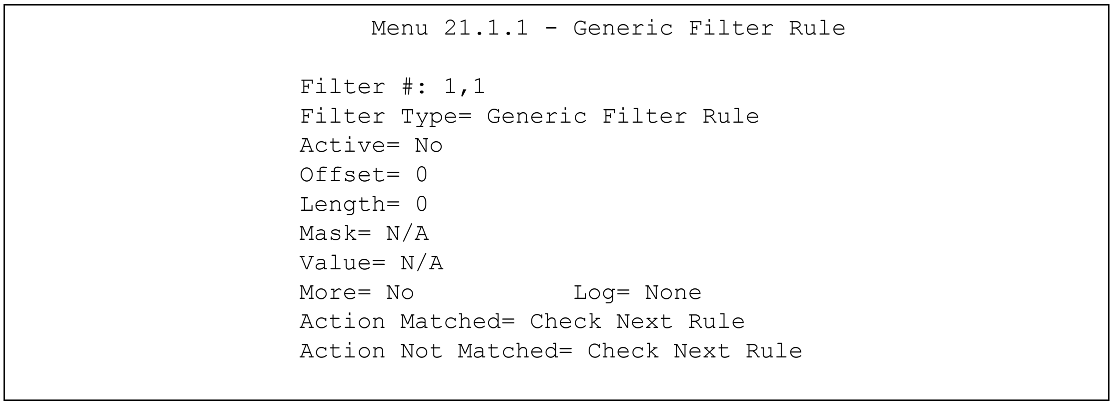
25.2.3 Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the ZyXEL Device treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The ZyXEL Device applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, `FFFFFFFF`.

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.1 and press [ENTER] to open Generic Filter Rule. Menu 21.1.1 is shown below as an example.

Figure 141 Menu 21.1.1: Generic Filter Rule



```
                    Menu 21.1.1 - Generic Filter Rule

               Filter #: 1,1
               Filter Type= Generic Filter Rule
               Active= No
               Offset= 0
               Length= 0
               Mask= N/A
               Value= N/A
               More= No            Log= None
               Action Matched= Check Next Rule
               Action Not Matched= Check Next Rule
```

The following table describes the fields in the **Generic Filter Rule** menu.

Table 78 Menu 21.1.1: Generic Filter Rule

FIELD	DESCRIPTION
Filter #	This is the filter set, filter rule co-ordinates, in other words 2,3 refers to the second filter set and the third rule of that set.
Filter Type	Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets. Options are **Generic Filter Rule** and **TCP/IP Filter Rule**.
Active	Select **Yes** to turn on the filter rule or **No** to turn it off.
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.
Mask	Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.
Value	Enter the value (in Hexadecimal notation) to compare with the data portion.
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If **More** is **Yes**, then Action Matched and Action Not Matched will be **No**.
Log	Select the logging option from the following: **None** - No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.

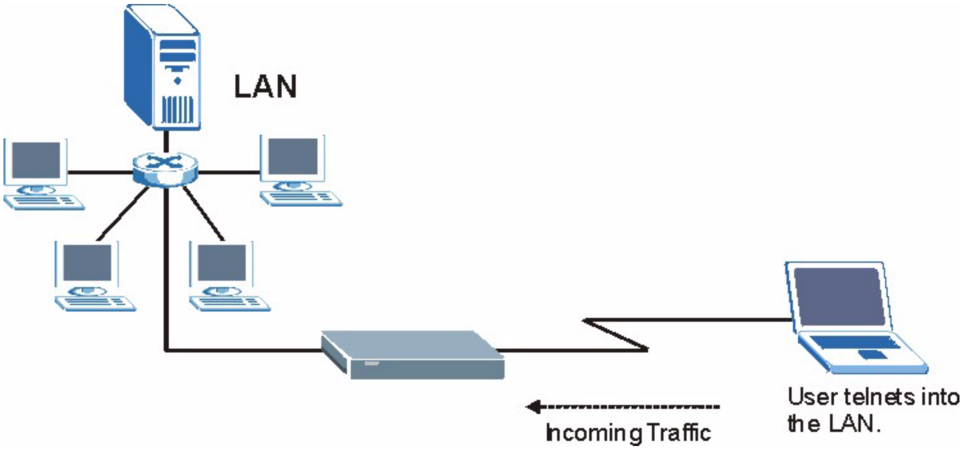
Table 78 Menu 21.1.1: Generic Filter Rule (continued)

FIELD	DESCRIPTION
Action Matched	Select the action for a packet matching the rule. Options are **Check Next Rule**, **Forward** and **Drop**.
Action Not Matched	Select the action for a packet not matching the rule. Options are **Check Next Rule**, **Forward** and **Drop**.
Once you have completed filling in **Menu 21.1.1 - Generic Filter Rule**, press [ENTER] at the message “Press ENTER to Confirm” to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1 - Filter Rules Summary**.	

25.3 Example Filter

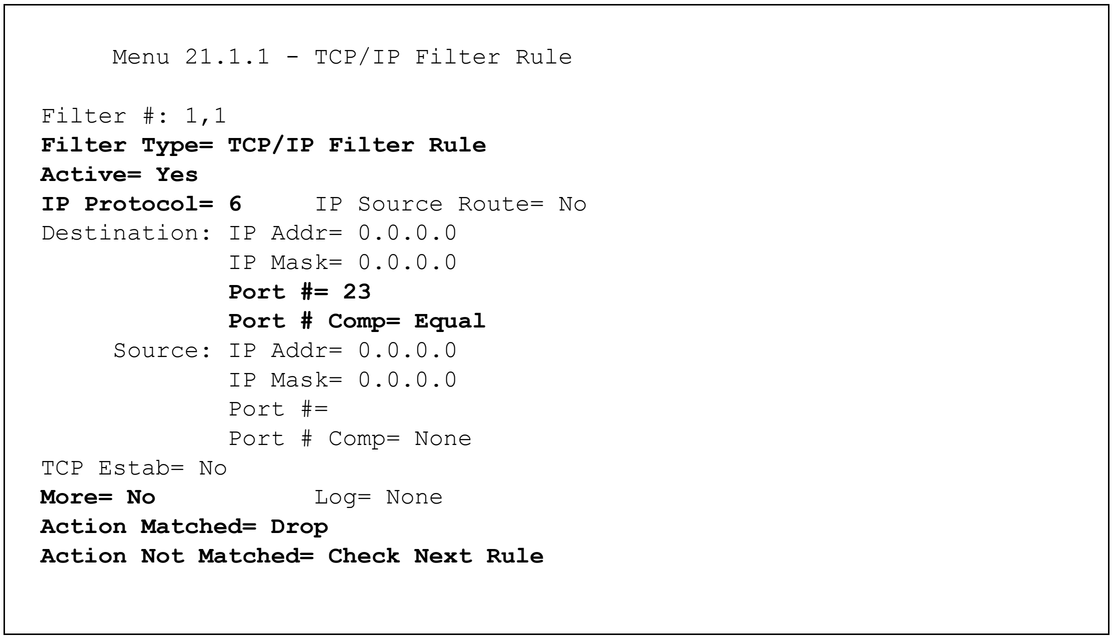
Let’s look at an example to block outside users from accessing the ZyXEL Device via telnet. Please see our included disk for more example filters.

Figure 142 Telnet Filter Example



1. Enter 21 from the main menu to open **Menu 21 - Filter Set Configuration**.
2. Enter the index of the filter set you wish to configure (say 3) and press [ENTER].
3. Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
4. Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1 - Filter Rules Summary**.
5. Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

Figure 143 Example Filter: Menu 21.1.1

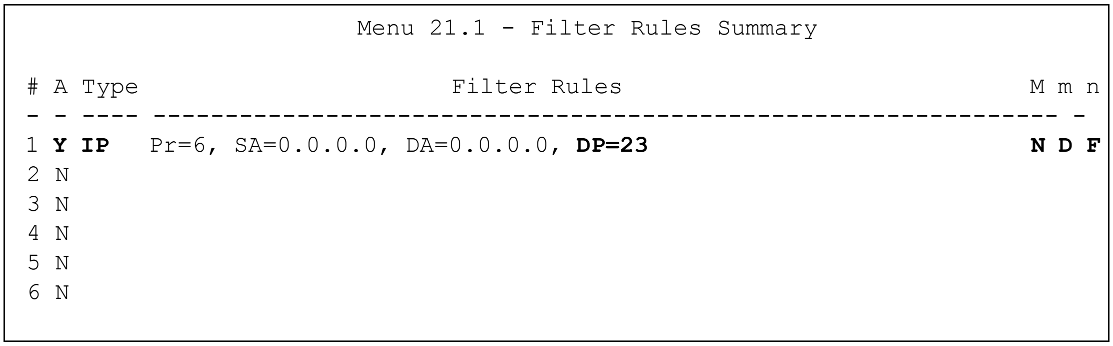


```
     Menu 21.1.1 - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6     IP Source Route= No
Destination: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 23
             Port # Comp= Equal
     Source: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #=
             Port # Comp= None
TCP Estab= No
More= No           Log= None
Action Matched= Drop
Action Not Matched= Check Next Rule
```

The port number for the telnet service (TCP protocol) is **23**. See *RFC 1060* for port numbers of well-known services.

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.

Figure 144 Example Filter Rules Summary: Menu 21.1.



```
                       Menu 21.1 - Filter Rules Summary

# A Type                      Filter Rules                            M m n
- - ---- --------------------------------------------------------------- -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                          N D F
2 N
3 N
4 N
5 N
6 N
```

This shows you that you have configured and activated (**A** = **Y**) a TCP/IP filter rule (**Type** = **IP**, **Pr** = **6**) for destination telnet ports (**DP** = **23**).

M = **N** means an action can be taken immediately. The action is to drop the packet (**m** = **D**) if the action is matched and to forward the packet immediately (**n** = **F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

After you've created the filter set, you must apply it.

1 Enter 11 from the main menu to go to menu 11.
2 Enter 1 or 2 to open **Menu 11.x - Remote Node Profile**.
3 Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].

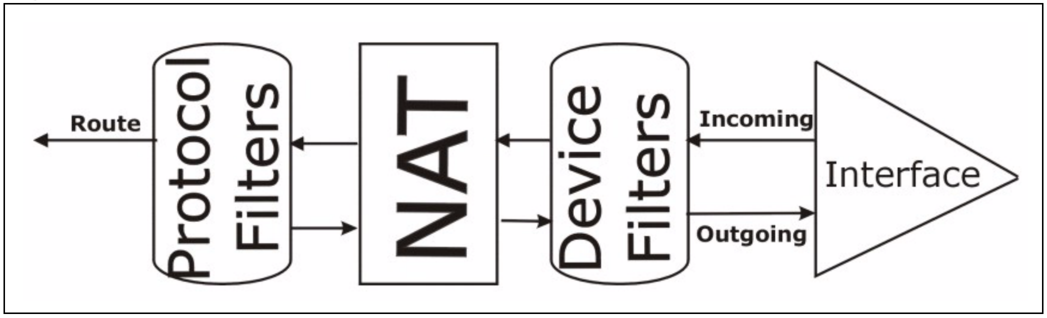
4 This brings you to menu 11.1.4. Apply a filter set (our example filter set 3) as shown in Figure 108 on page 191.

5 Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.1.4.

25.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and protocol filter (**TCP/IP**) rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ZyXEL Device applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the ZyXEL Device is receiving and sending the packets; in other words the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

Figure 145 Protocol and Device Filter Sets



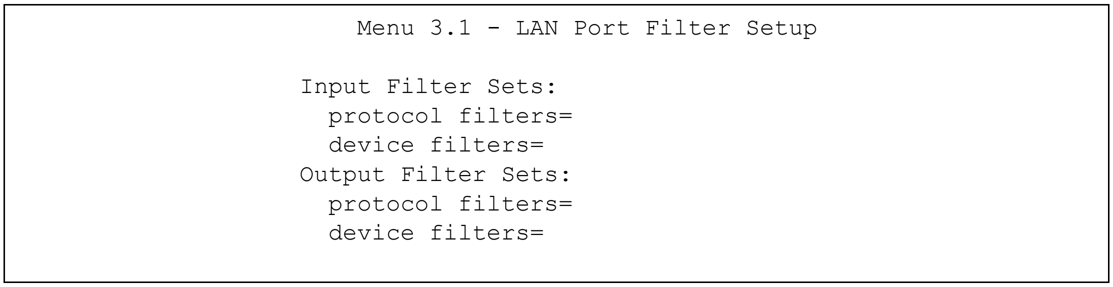
25.5 Applying a Filter

This section shows you where to apply the filter(s) after you design it (them). The ZyXEL Device already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

25.5.1 Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, for example 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyXEL Device and output filter sets filter outgoing traffic from the ZyXEL Device.

Figure 146 Filtering LAN Traffic

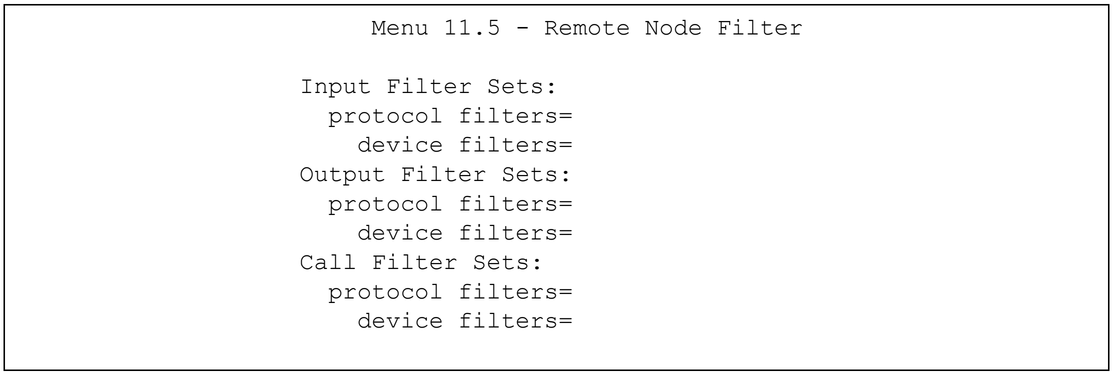


```
                        Menu 3.1 - LAN Port Filter Setup

                    Input Filter Sets:
                      protocol filters=
                      device filters=
                    Output Filter Sets:
                      protocol filters=
                      device filters=
```

25.5.2 Applying Remote Node Filters

Go to menu 11.5 (shown below – note that call filter sets are only present for PPPoA or PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The ZyXEL Device already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

Figure 147 Filtering Remote Node Traffic



```
                         Menu 11.5 - Remote Node Filter

                    Input Filter Sets:
                      protocol filters=
                        device filters=
                    Output Filter Sets:
                      protocol filters=
                        device filters=
                    Call Filter Sets:
                      protocol filters=
                        device filters=
```

26

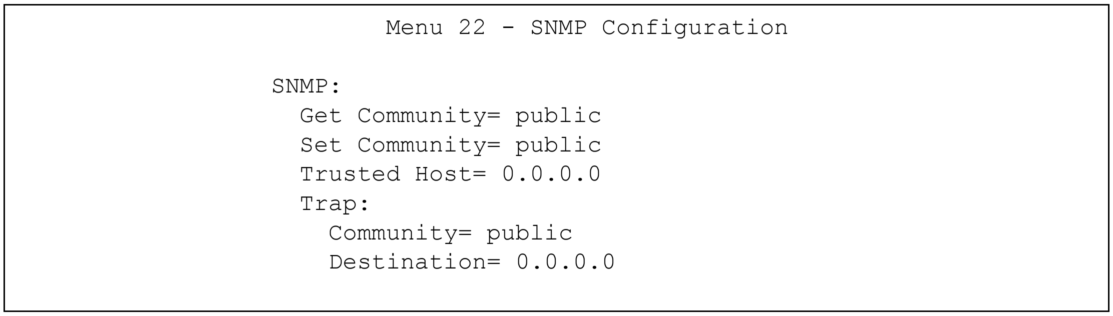
SNMP Configuration

Use this menu to configure SNMP. See Section 11.6 on page 122 for more information about SNMP.

26.1 SNMP Configuration

To configure SNMP, enter 22 from the main menu to display **Menu 22 - SNMP Configuration** as shown next. The “community” for **Get**, **Set** and **Trap** fields is SNMP terminology for password.

Figure 148 Menu 22: SNMP Configuration



```
                          Menu 22 - SNMP Configuration

                  SNMP:
                    Get Community= public
                    Set Community= public
                    Trusted Host= 0.0.0.0
                    Trap:
                      Community= public
                      Destination= 0.0.0.0
```

The following table describes the SNMP configuration parameters.

Table 79 Menu 22: SNMP Configuration

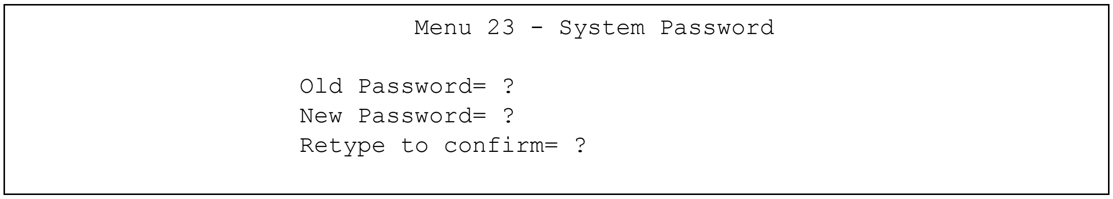
FIELD	DESCRIPTION
Get Community	Type the Get community, which is the password for the incoming Get- and GetNext requests from the management station.
Set Community	Type the Set community, which is the password for incoming Set requests from the management station.
Trusted Host	If you enter a trusted host, your ZyXEL Device will only respond to SNMP messages from this address. A blank (default) field means your ZyXEL Device will respond to all SNMP messages it receives, regardless of source.
Trap	
Community	Type the Trap community, which is the password sent with each trap to the SNMP manager.
Destination	Type the IP address of the station to send your SNMP traps to.
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

27

System Password

Use this menu to change your password. This is the same password used to access the web configurator. To open this menu, enter 23 in the main menu.

Figure 149 Menu 23: System Password



```
                         Menu 23 - System Password

                 Old Password= ?
                 New Password= ?
                 Retype to confirm= ?
```

The following table describes the labels in this menu.

Table 80 Menu 23: System Password

FIELD	DESCRIPTION
Old Password	Enter the current administrator password for the ZyXEL Device.
New Password	Enter the new administrator password for the ZyXEL Device.
Retype to confirm	Enter the new administrator password again.

28

System Information & Diagnosis

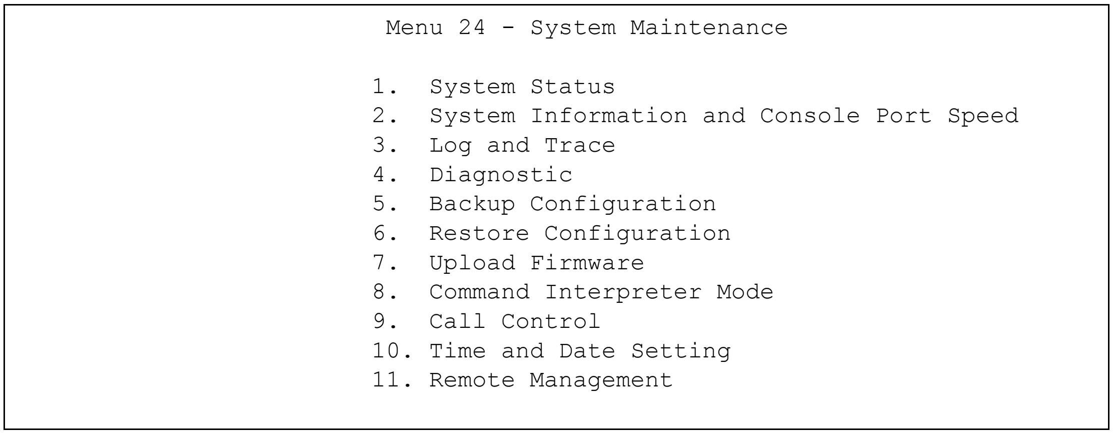
This chapter covers SMT menus 24.1 to 24.4.

28.1 Introduction to System Status

This chapter covers the diagnostic tools that help you to maintain your ZyXEL Device. These tools include updates on system status, port status and log and trace capabilities.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance, as shown below.**

Figure 150 Menu 24: System Maintenance



```
                          Menu 24 - System Maintenance

                         1.   System Status
                         2.   System Information and Console Port Speed
                         3.   Log and Trace
                         4.   Diagnostic
                         5.   Backup Configuration
                         6.   Restore Configuration
                         7.   Upload Firmware
                         8.   Command Interpreter Mode
                         9.   Call Control
                         10.  Time and Date Setting
                         11.  Remote Management
```

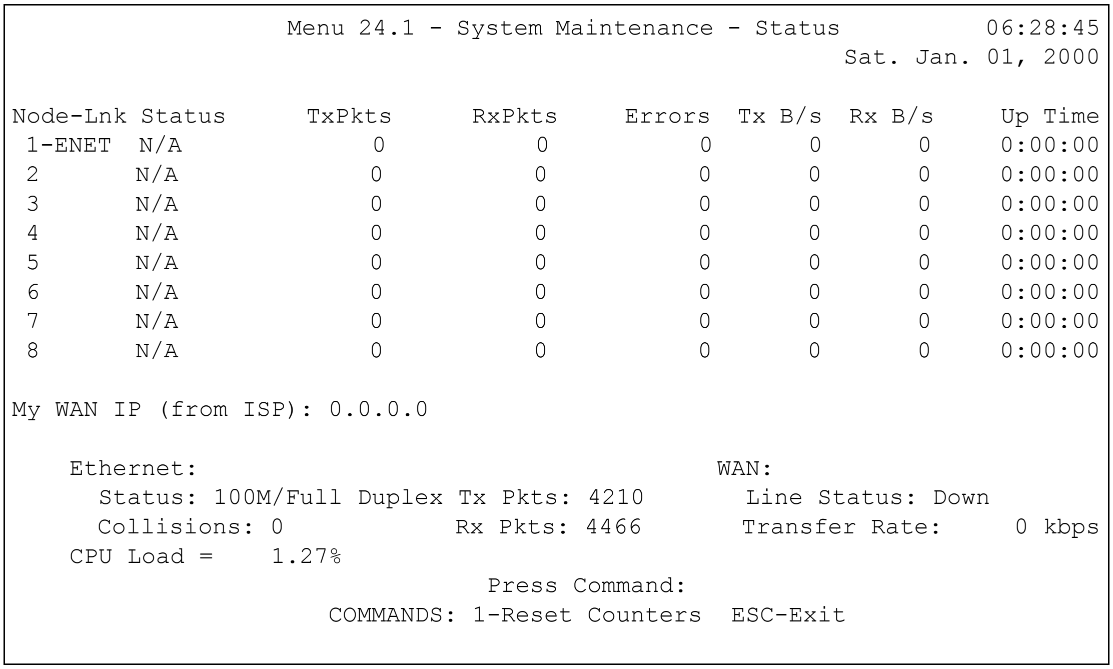
28.2 System Status

The first selection, System Status, gives you information on the version of your system firmware and the status and statistics of the ports, as shown in the next figure. System Status is a tool that can be used to monitor your ZyXEL Device. Specifically, it gives you information on your system firmware version, number of packets sent and number of packets received.

To get to the System Status:

1. Enter number 24 to go to Menu 24 - System Maintenance.
2. In this menu, enter 1 to open System Maintenance - Status.
3. There are three commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 drops the WAN connection, 9 resets the counters and [ESC] takes you back to the previous screen.

Figure 151 Menu 24.1: System Maintenance - Status



```
                    Menu 24.1 - System Maintenance - Status          06:28:45
                                                               Sat. Jan. 01, 2000

Node-Lnk Status      TxPkts      RxPkts     Errors  Tx B/s  Rx B/s     Up Time
 1-ENET  N/A              0           0          0       0       0     0:00:00
 2       N/A              0           0          0       0       0     0:00:00
 3       N/A              0           0          0       0       0     0:00:00
 4       N/A              0           0          0       0       0     0:00:00
 5       N/A              0           0          0       0       0     0:00:00
 6       N/A              0           0          0       0       0     0:00:00
 7       N/A              0           0          0       0       0     0:00:00
 8       N/A              0           0          0       0       0     0:00:00

My WAN IP (from ISP): 0.0.0.0

    Ethernet:                                      WAN:
      Status: 100M/Full Duplex Tx Pkts: 4210         Line Status: Down
      Collisions: 0            Rx Pkts: 4466         Transfer Rate:     0 kbps
    CPU Load =    1.27%
                                  Press Command:
                       COMMANDS: 1-Reset Counters  ESC-Exit
```

The following table describes the fields present in **Menu 24.1 - System Maintenance - Status**. These fields are read-only and meant for diagnostic purposes. The upper right corner of the screen shows the time and date.

Table 81 Menu 24.1: System Maintenance - Status

FIELD	DESCRIPTION
Node-Lnk	This field is the remote node index number and link type (encapsulation).
Status	This field displays **Down** (line is down), **Up** (line is up or connected) if you're using Ethernet encapsulation and **Down** (line is down), **Up** (line is up or connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation. It displays **N/A** if the port is not connected.
TxPkts	This is the number of packets transmitted from the ZyXEL Device to the remote node.
RxPkts	This is the number of packets received by the ZyXEL Device from the remote node.
Errors	This is the number of error packets on this connection.
Tx B/s	This field shows the transmission rate in bytes per second on this port.
Rx B/s	This field shows the reception rate in bytes per second on this port.
Up Time	This is the total amount of time the this channel has been connected to the remote node.
My WAN IP (from ISP)	This is the IP address assigned by your ISP or the static IP address you set up in menu 4.
Ethernet:	This section displays information about the LAN ports.
Status	This field displays the speed and duplex settings of the LAN ports.
Collisions	This is the number of collisions on this port.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.

Table 81 Menu 24.1: System Maintenance - Status (continued)

FIELD	DESCRIPTION
WAN	This section displays information about the WAN port. Note: In a point-to-2points connection this field only displays line 1 status.
Line Status	This field displays the port speed and duplex setting if you're using Ethernet encapsulation and **Down** (line is down or not connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) or **Drop** (dropping a call) if you're using PPPoE encapsulation.
Transfer Rate	This field shows the transmission speed in kilobits per second on this port.
CPU Load	This field displays the percentage of CPU utilization.
You may enter 1 to reset the counters or [ESC] to return to menu 24.	

28.3 System Information and Console Port Speed

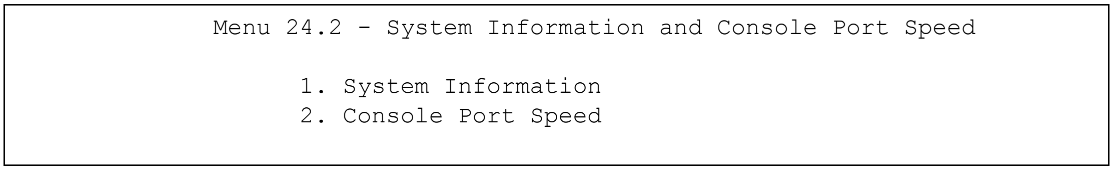
This section describes your system and allows you to choose different console port speeds. To get to the System Information and Console Port Speed:

1 Enter 24 to go to **Menu 24 - System Maintenance**.

2 Enter 2 to open **Menu 24.2 - System Information and Console Port Speed**.

3 From this menu you have two choices as shown in the next figure:

Figure 152 Menu 24.2: System Information and Console Port Speed

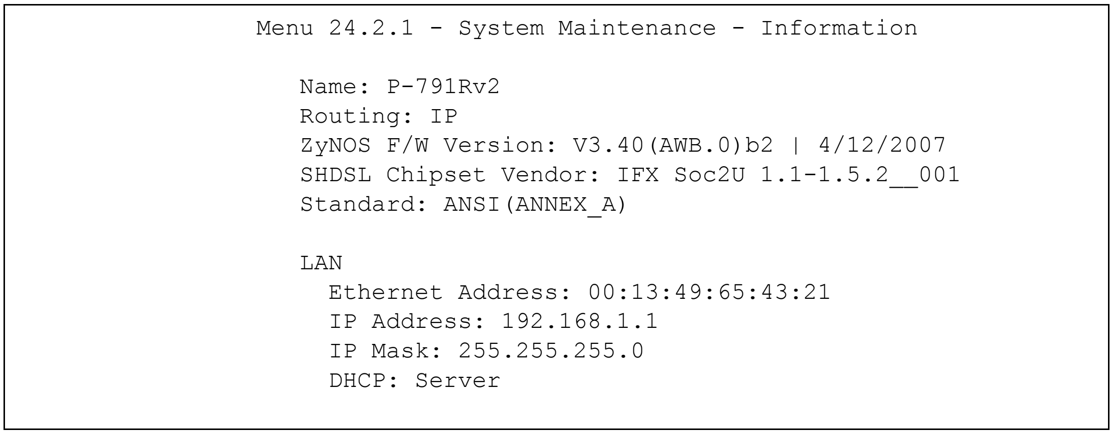


```
              Menu 24.2 - System Information and Console Port Speed

                    1. System Information
                    2. Console Port Speed
```

28.3.1 System Information

System Information gives you information about your system as shown below. More specifically, it gives you information on your routing protocol, Ethernet address, IP address, etc.

Figure 153 Menu 24.2.1: System Maintenance - Information



```
                  Menu 24.2.1 - System Maintenance - Information

                     Name: P-791Rv2
                     Routing: IP
                     ZyNOS F/W Version: V3.40(AWB.0)b2 | 4/12/2007
                     SHDSL Chipset Vendor: IFX Soc2U 1.1-1.5.2__001
                     Standard: ANSI(ANNEX_A)

                     LAN
                       Ethernet Address: 00:13:49:65:43:21
                       IP Address: 192.168.1.1
                       IP Mask: 255.255.255.0
                       DHCP: Server
```

The following table describes the fields in this screen.

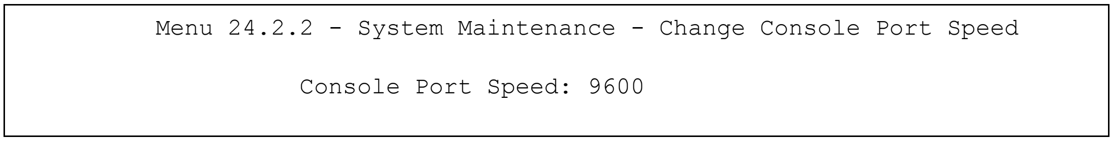
Table 82 Menu 24.2.1: System Maintenance - Information

FIELD	DESCRIPTION
Name	This is the ZyXEL Device's system name + domain name assigned in menu 1. For example, System Name= xxx; Domain Name= baboo.mickey.com Name= xxx.baboo.mickey.com
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the version of ZyXEL's Network Operating System software.
SHDSL Chipset Vendor	Refers to the SHDSL chipset inside the ZyXEL Device.
Standard	This refers to the operational protocol the ZyXEL Device and DSLAM (Digital Subscriber Line Access Multiplexer) are using.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) address of your ZyXEL Device.
IP Address	This is the IP address of the ZyXEL Device in dotted decimal notation.
IP Mask	This shows the IP mask of the ZyXEL Device.
DHCP	This field shows the DHCP setting of the ZyXEL Device.
When finished viewing, press [ESC] or [ENTER] to exit.	

28.3.2 Console Port Speed

You can change the speed of the console port through **Menu 24.2.2 – System Maintenance - Change Console Port Speed**. Your ZyXEL Device supports 9600 (default), 19200, 38400, 57600, and 115200 bps for the console port. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown next.

Figure 154 Menu 24.2.2: System Maintenance: Change Console Port Speed



```
           Menu 24.2.2 - System Maintenance - Change Console Port Speed

                     Console Port Speed: 9600
```

28.4 Log and Trace

There are two logging facilities in the ZyXEL Device. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

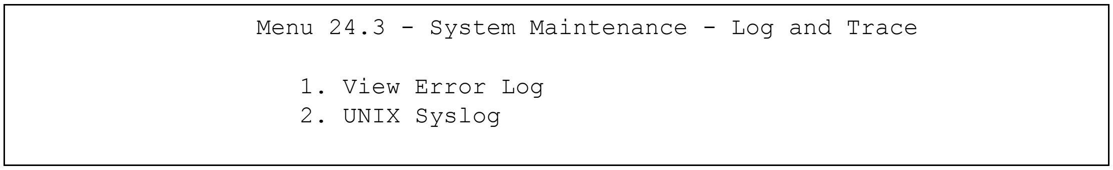
28.4.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error/trace log. Follow the procedure below to view the local error/trace log:

1. Select option 24 from the main menu to open **Menu 24 - System Maintenance**.
2. From menu 24, select option 3 to open **Menu 24.3 - System Maintenance - Log and Trace**.
3. Select the first option from **Menu 24.3 - System Maintenance - Log and Trace** to display the error log in the system.

After the ZyXEL Device finishes displaying, you will have the option to clear the error log.

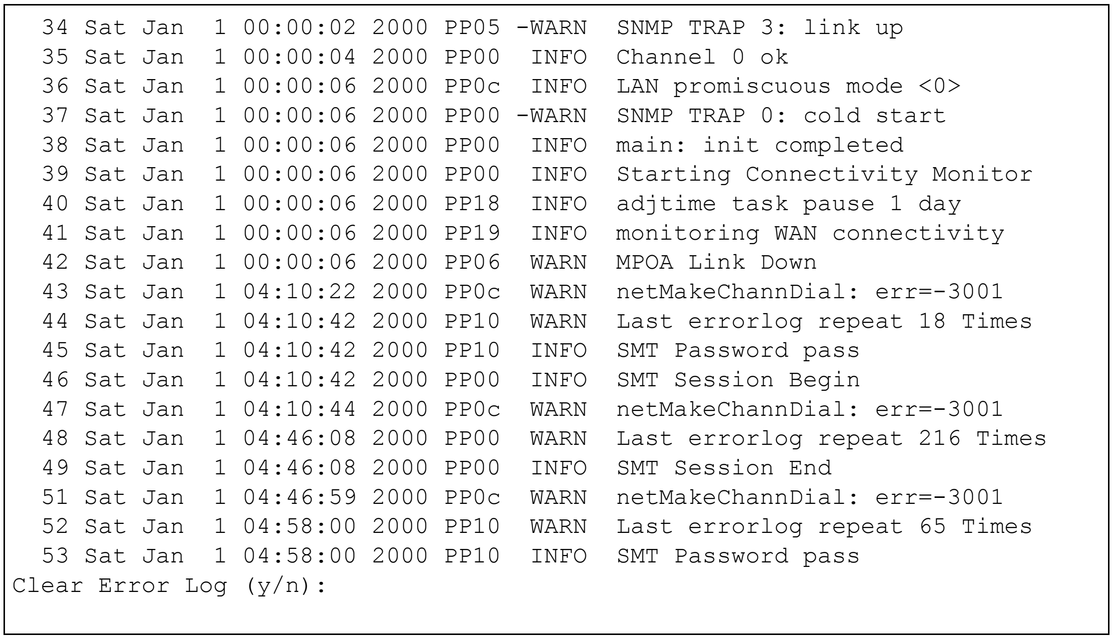
Figure 155 Menu 24.3: System Maintenance - Log and Trace



```
                 Menu 24.3 - System Maintenance - Log and Trace

                    1. View Error Log
                    2. UNIX Syslog
```

Examples of typical error and information messages are presented in the following figure.

Figure 156 Examples of Error and Information Messages

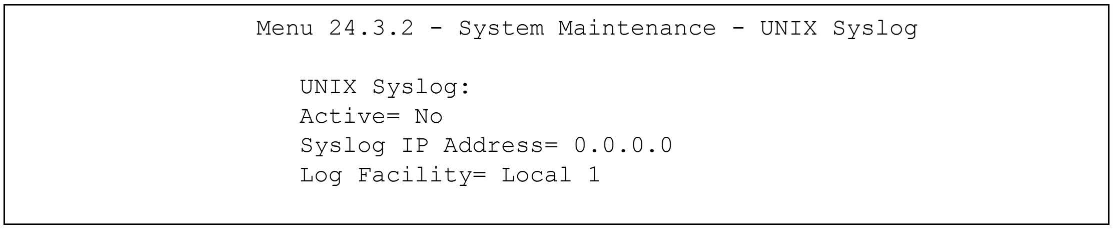


```
  34 Sat Jan  1 00:00:02 2000 PP05 -WARN  SNMP TRAP 3: link up
  35 Sat Jan  1 00:00:04 2000 PP00  INFO  Channel 0 ok
  36 Sat Jan  1 00:00:06 2000 PP0c  INFO  LAN promiscuous mode <0>
  37 Sat Jan  1 00:00:06 2000 PP00 -WARN  SNMP TRAP 0: cold start
  38 Sat Jan  1 00:00:06 2000 PP00  INFO  main: init completed
  39 Sat Jan  1 00:00:06 2000 PP00  INFO  Starting Connectivity Monitor
  40 Sat Jan  1 00:00:06 2000 PP18  INFO  adjtime task pause 1 day
  41 Sat Jan  1 00:00:06 2000 PP19  INFO  monitoring WAN connectivity
  42 Sat Jan  1 00:00:06 2000 PP06  WARN  MPOA Link Down
  43 Sat Jan  1 04:10:22 2000 PP0c  WARN  netMakeChannDial: err=-3001
  44 Sat Jan  1 04:10:42 2000 PP10  WARN  Last errorlog repeat 18 Times
  45 Sat Jan  1 04:10:42 2000 PP10  INFO  SMT Password pass
  46 Sat Jan  1 04:10:42 2000 PP00  INFO  SMT Session Begin
  47 Sat Jan  1 04:10:44 2000 PP0c  WARN  netMakeChannDial: err=-3001
  48 Sat Jan  1 04:46:08 2000 PP00  WARN  Last errorlog repeat 216 Times
  49 Sat Jan  1 04:46:08 2000 PP00  INFO  SMT Session End
  51 Sat Jan  1 04:46:59 2000 PP0c  WARN  netMakeChannDial: err=-3001
  52 Sat Jan  1 04:58:00 2000 PP10  WARN  Last errorlog repeat 65 Times
  53 Sat Jan  1 04:58:00 2000 PP10  INFO  SMT Password pass
Clear Error Log (y/n):
```

28.4.2 Syslog Logging

The ZyXEL Device uses the syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 - System Maintenance - Syslog Logging**, as shown next.

Figure 157 Menu 24.3.2: System Maintenance - UNIX Syslog



```
                  Menu 24.3.2 - System Maintenance - UNIX Syslog

                     UNIX Syslog:
                     Active= No
                     Syslog IP Address= 0.0.0.0
                     Log Facility= Local 1
```

You need to configure the syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 83 Menu 24.3.2: System Maintenance - UNIX Syslog

FIELD	DESCRIPTION
UNIX Syslog:	
Active	Press [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Press [SPACE BAR] and then [ENTER] to select a location. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

Your ZyXEL Device sends five types of syslog messages. Some examples (not all ZyXEL Device specific) of these syslog messages with their message formats are shown next:

1 CDR

CDR Message Format
SdcmdSyslogSend(SYSLOG_CDR, SYSLOG_INFO, String); String = board xx line xx channel xx, call xx, str board = the hardware board ID line = the WAN ID in a board Channel = channel ID within the WAN call = the call reference number which starts from 1 and increments by 1 for each new call str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.) L02 Tunnel Connected(L2TP) C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number) L02 Call Terminated C02 Call Terminated Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002 Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002 Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated

2 Packet triggered

Packet triggered Message Format

SdcmdSyslogSend(SYSLOG_PKTTRI, SYSLOG_NOTICE, String);
String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
Data: We will send forty-eight Hex characters to the server

Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000

3 Filter log

Filter log Message Format
SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String);
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD
IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D).
Src: Source Address
Dst: Destination Address
prot: Protocol ("TCP","UDP","ICMP")
spo: Source port
dpo: Destination portMar 03 10:39:43 202.132.155.97 ZyXEL: GEN[ffffffffffffnordff0080] }S05>R01mF
Mar 03 10:41:29 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 10:41:34 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF
Mar 03 11:59:20 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 12:00:52 202.132.155.97 ZyXEL:
GEN[ffffffffffff0080] }S05>R01mF
Mar 03 12:00:57 202.132.155.97 ZyXEL:
GEN[00a0c5f502010080] }S05>R01mF
Mar 03 12:01:06 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021]}S04>R01mF

4 PPP log

PPP Log Message Format
SdcmdSyslogSend(SYSLOG_PPPLOG, SYSLOG_NOTICE, String); String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing

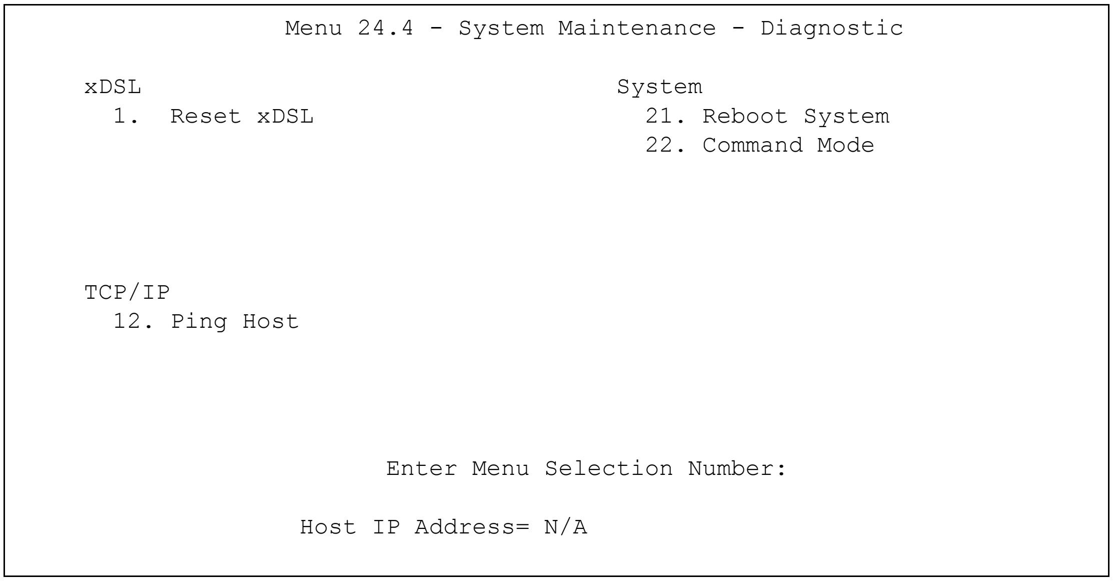
28.5 Diagnostic

The diagnostic facility allows you to test the different aspects of your ZyXEL Device to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown next. Not all fields are available on all models.

Follow the procedure below to get to **Menu 24.4 - System Maintenance - Diagnostic**.

1. From the main menu, select option 24 to open **Menu 24 - System Maintenance**.
2. From this menu, select option 4. Diagnostic. This will open **Menu 24.4 - System Maintenance - Diagnostic**.

Figure 158 Menu 24.4: System Maintenance - Diagnostic



```
                Menu 24.4 - System Maintenance - Diagnostic

     xDSL                                 System
       1.  Reset xDSL                       21. Reboot System
                                            22. Command Mode




     TCP/IP
       12. Ping Host




                       Enter Menu Selection Number:

                 Host IP Address= N/A
```

The following table describes the labels in this screen.

Table 84 Menu 24.4: System Maintenance - Diagnostic

FIELD	DESCRIPTION
Reset xDSL	Enter 1 to reset the DSL connection on the WAN port.
Ping Host	Enter 12 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the **Host IP Address** field below.
Reboot System	Enter 11 to reboot the ZyXEL Device.
Command Mode	Enter 22 to go to the Command Interpreter (CI) for further diagnosis. You can also enter the CI using menu 24.8.
Host IP Address	If you entered 1in the **Enter Menu Selection Number** field, then enter the IP address of the computer you want to ping in this field.
Enter the number of the selection you would like to perform or press [ESC] to cancel.	

29

Firmware and Configuration File Maintenance

This chapter tells you how to back up and restore your configuration file as well as upload new firmware and a new configuration file.

29.1 Introduction

Use the instructions in this chapter to change the ZyXEL Device's configuration file or upgrade its firmware. After you configure your ZyXEL Device, you can backup the configuration file to a computer. That way if you later misconfigure the ZyXEL Device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the ZyXEL Device to the original default settings. The firmware determines the ZyXEL Device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site to use to upgrade your ZyXEL Device's performance.

29.2 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the ZyXEL Device's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the ZyXEL Device.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file "config.cfg".

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyXEL Device only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyXEL Device and the external filename refers to the filename not on the ZyXEL Device, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **ZyNOS F/W Version** field in **Menu 24.2.1 - System Maintenance - Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press "y" when prompted in the SMT menu to go into debug mode.

Table 85 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the ZyXEL Device. Uploading the rom-0 file replaces the entire ROM file system, including your ZyXEL Device configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the ZyXEL Device.	*.bin

29.3 Backup Configuration

The ZyXEL Device displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2 depending on whether you use the console port or Telnet.

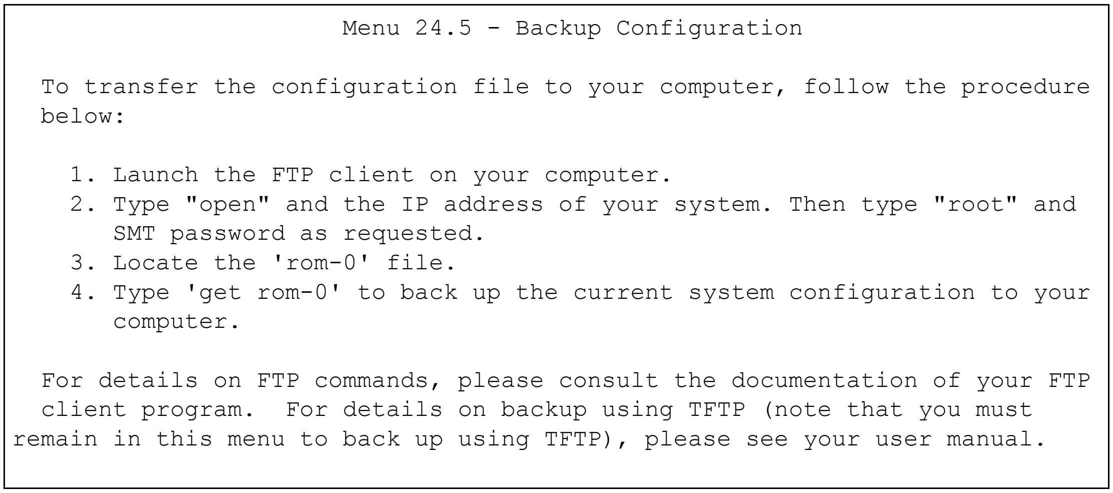
Option 5 from **Menu 24 - System Maintenance** allows you to backup the current ZyXEL Device configuration to your computer. Backup is highly recommended once your ZyXEL Device is functioning properly. FTP is the preferred method for backing up your current configuration to your computer since it is faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

Please note that terms "download" and "upload" are relative to the computer. Download means to transfer from the ZyXEL Device to the computer, while upload means from your computer to the ZyXEL Device.

29.3.1 Backup Configuration

Follow the instructions as shown in the next screen.

Figure 159 Menu 24.5: Backup Configuration



```
                       Menu 24.5 - Backup Configuration

  To transfer the configuration file to your computer, follow the procedure
  below:

    1. Launch the FTP client on your computer.
    2. Type "open" and the IP address of your system. Then type "root" and
       SMT password as requested.
    3. Locate the 'rom-0' file.
    4. Type 'get rom-0' to back up the current system configuration to your
       computer.

  For details on FTP commands, please consult the documentation of your FTP
  client program.  For details on backup using TFTP (note that you must
remain in this menu to back up using TFTP), please see your user manual.
```

29.3.2 Using the FTP Command from the Command Line

1 Launch the FTP client on your computer.

2 Enter “open”, followed by a space and the IP address of your ZyXEL Device.

3 Press [ENTER] when prompted for a username.

4 Enter your password as requested (the default is “1234”).

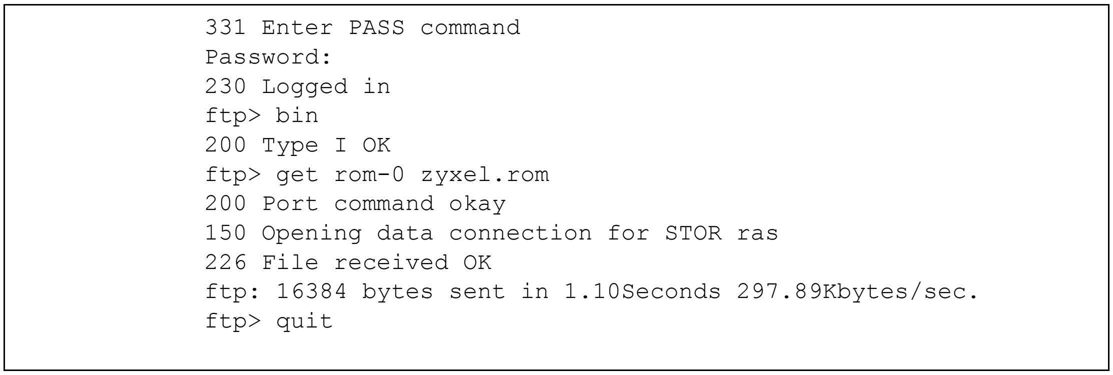
5 Enter “bin” to set transfer mode to binary.

6 Use “get” to transfer files from the ZyXEL Device to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the ZyXEL Device to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.

7 Enter “quit” to exit the ftp prompt.

29.3.3 Example of FTP Commands from the Command Line

Figure 160 FTP Session Example



```
              331 Enter PASS command
              Password:
              230 Logged in
              ftp> bin
              200 Type I OK
              ftp> get rom-0 zyxel.rom
              200 Port command okay
              150 Opening data connection for STOR ras
              226 File received OK
              ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
              ftp> quit
```

29.3.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 86 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

29.3.5 File Maintenance Over WAN

TFTP, FTP and Telnet over the WAN will not work when:

1. You have disabled Telnet service in menu 24.11.
2. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
3. The IP you entered in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the ZyXEL Device will disconnect the Telnet session immediately.
4. You have an SMT console session running.

29.3.6 Backup Configuration Using TFTP

The ZyXEL Device supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the ZyXEL Device and log in. Because TFTP does not have any security checks, the ZyXEL Device records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
3. Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
4. Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.

5 Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the configuration file is “rom-0” (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyXEL Device to the computer and “binary” to set binary transfer mode.

29.3.7 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyXEL Device IP address, “get” transfers the file source on the ZyXEL Device (rom-0, name of the configuration file on the ZyXEL Device) to the file destination on the computer and renames it config.rom.

29.3.8 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 87 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyXEL Device. 192.168.1.1 is the ZyXEL Device’s default IP address when shipped.
Send/Fetch	Use “Send” to upload the file to the ZyXEL Device and “Fetch” to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyXEL Device. The filename for the firmware is “ras” and for the configuration file, is “rom-0”.
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

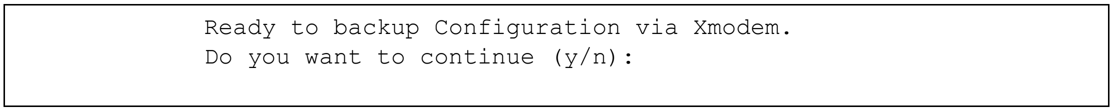
Refer to Section 29.3.5 on page 244 to read about configurations that disallow TFTP and FTP over WAN.

29.3.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

1 Display menu 24.5 and enter “y” at the following screen.

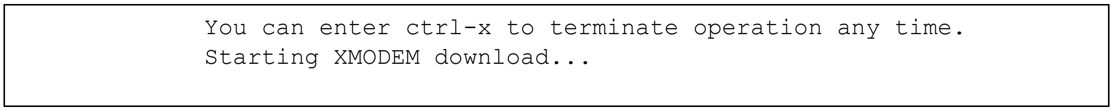
Figure 161 System Maintenance: Backup Configuration



```
               Ready to backup Configuration via Xmodem.
               Do you want to continue (y/n):
```

2 The following screen indicates that the Xmodem download has started.

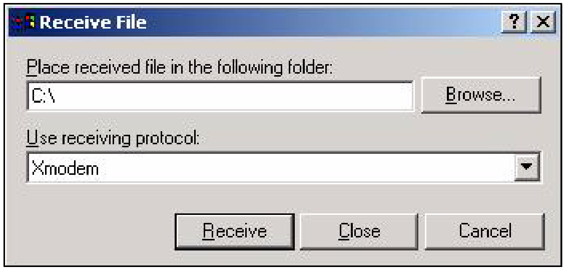
Figure 162 System Maintenance: Starting Xmodem Download Screen



```
You can enter ctrl-x to terminate operation any time.
Starting XMODEM download...
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

Figure 163 Backup Configuration Example



Place received file in the following folder: C:\

Use receiving protocol: Xmodem

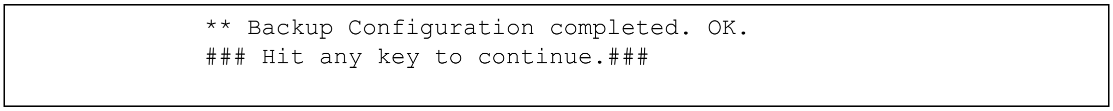
Type a location for storing the configuration file or click **Browse** to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

4 After a successful backup you will see the following screen. Press any key to return to the SMT menu.

Figure 164 Successful Backup Confirmation Screen



```
** Backup Configuration completed. OK.
### Hit any key to continue.###
```

29.4 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

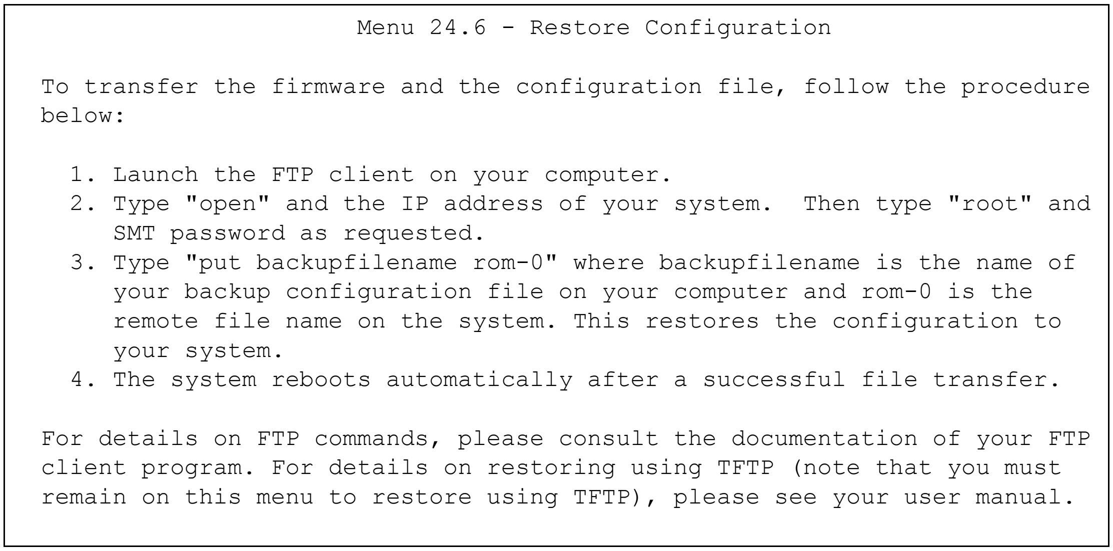
FTP is the preferred method for restoring your current computer configuration to your ZyXEL Device since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyXEL Device. When the Restore Configuration process is complete, the ZyXEL Device will automatically restart.

29.4.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

Figure 165 Menu 24.6: Restore Configuration

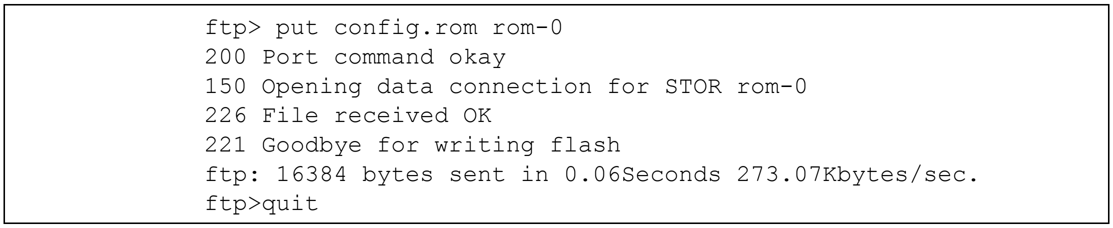


```
                       Menu 24.6 - Restore Configuration

To transfer the firmware and the configuration file, follow the procedure
below:

  1. Launch the FTP client on your computer.
  2. Type "open" and the IP address of your system.  Then type "root" and
     SMT password as requested.
  3. Type "put backupfilename rom-0" where backupfilename is the name of
     your backup configuration file on your computer and rom-0 is the
     remote file name on the system. This restores the configuration to
     your system.
  4. The system reboots automatically after a successful file transfer.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on restoring using TFTP (note that you must
remain on this menu to restore using TFTP), please see your user manual.
```

1 Launch the FTP client on your computer.
2 Enter “open”, followed by a space and the IP address of your ZyXEL Device.
3 Press [ENTER] when prompted for a username.
4 Enter your password as requested (the default is “1234”).
5 Enter “bin” to set transfer mode to binary.
6 Find the “rom” file (on your computer) that you want to restore to your ZyXEL Device.
7 Use “put” to transfer files from the ZyXEL Device to the computer, for example, “put config.rom rom-0” transfers the configuration file “config.rom” on your computer to the ZyXEL Device. See earlier in this chapter for more information on filename conventions.
8 Enter “quit” to exit the ftp prompt. The ZyXEL Device will automatically restart after a successful restore process.

29.4.2 Restore Using FTP Session Example

Figure 166 Restore Using FTP Session Example



```
              ftp> put config.rom rom-0
              200 Port command okay
              150 Opening data connection for STOR rom-0
              226 File received OK
              221 Goodbye for writing flash
              ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
              ftp>quit
```

Refer to Section 29.3.5 on page 244 to read about configurations that disallow TFTP and FTP over WAN.

29.4.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

1 Display menu 24.6 and enter “y” at the following screen.

Figure 167 System Maintenance: Restore Configuration

```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

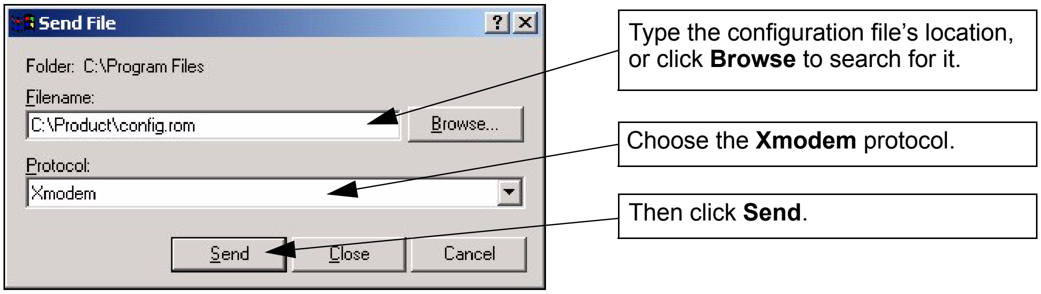
2 The following screen indicates that the Xmodem download has started.

Figure 168 System Maintenance: Starting Xmodem Download Screen

```
Starting XMODEM download (CRC mode) ...CCCCCCCCC
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

Figure 169 Restore Configuration Example



Filename: C:\Product\config.rom

Protocol: Xmodem

Type the configuration file’s location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

4 After a successful restoration you will see the following screen. Press any key to restart the ZyXEL Device and return to the SMT menu.

Figure 170 Successful Restoration Confirmation Screen

```
Save to ROM
Hit any key to start system reboot.
```

29.5 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in Section 29.4 on page 246 or by following the instructions in **Menu 24.7.2 - System Maintenance - Upload System Configuration File** (for console port).

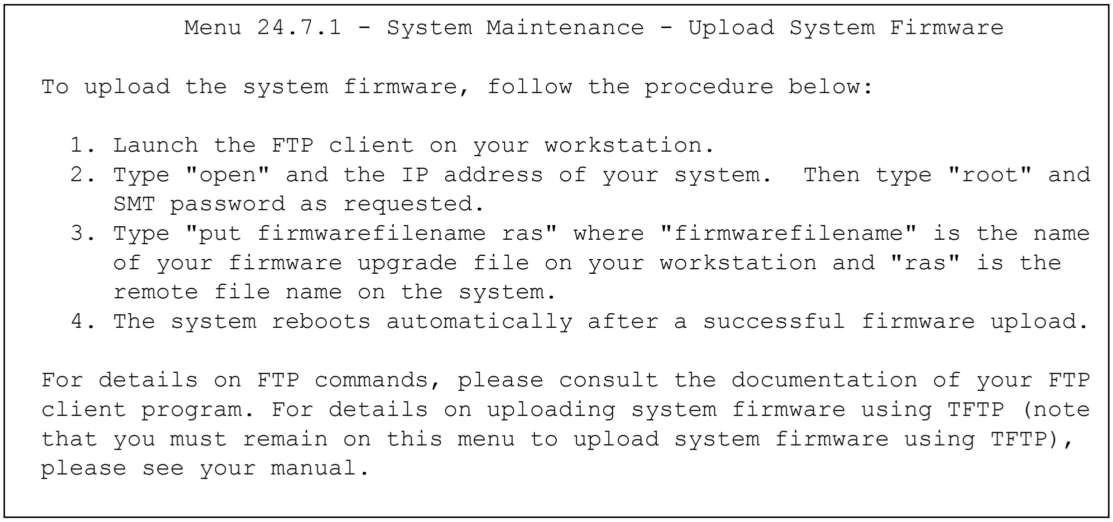
Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyXEL Device.

29.5.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the ZyXEL Device, you will see the following screens for uploading firmware and the configuration file using FTP.

Figure 171 Menu 24.7.1: System Maintenance - Upload System Firmware

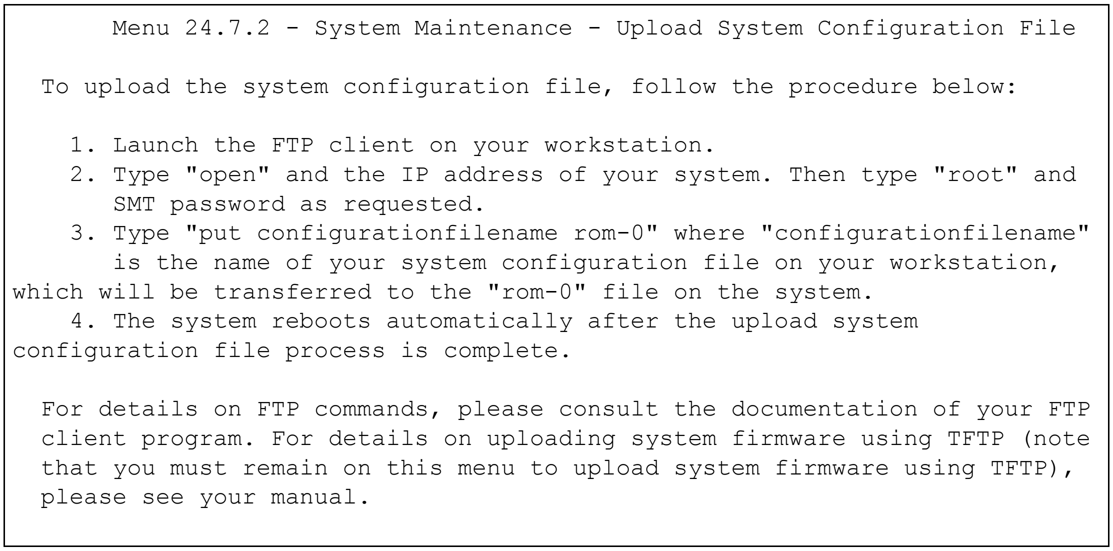


```
          Menu 24.7.1 - System Maintenance - Upload System Firmware

 To upload the system firmware, follow the procedure below:

   1. Launch the FTP client on your workstation.
   2. Type "open" and the IP address of your system.  Then type "root" and
      SMT password as requested.
   3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
      of your firmware upgrade file on your workstation and "ras" is the
      remote file name on the system.
   4. The system reboots automatically after a successful firmware upload.

 For details on FTP commands, please consult the documentation of your FTP
 client program. For details on uploading system firmware using TFTP (note
 that you must remain on this menu to upload system firmware using TFTP),
 please see your manual.
```

29.5.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

Figure 172 Menu 24.7.2: System Maintenance - Upload System Configuration File



```
      Menu 24.7.2 - System Maintenance - Upload System Configuration File

  To upload the system configuration file, follow the procedure below:

    1. Launch the FTP client on your workstation.
    2. Type "open" and the IP address of your system. Then type "root" and
       SMT password as requested.
    3. Type "put configurationfilename rom-0" where "configurationfilename"
       is the name of your system configuration file on your workstation,
which will be transferred to the "rom-0" file on the system.
    4. The system reboots automatically after the upload system
configuration file process is complete.

  For details on FTP commands, please consult the documentation of your FTP
  client program. For details on uploading system firmware using TFTP (note
  that you must remain on this menu to upload system firmware using TFTP),
  please see your manual.
```

To upload the firmware and the configuration file, follow these examples

29.5.3 FTP File Upload Command from the DOS Prompt Example

1 Launch the FTP client on your computer.

2 Enter “open”, followed by a space and the IP address of your ZyXEL Device.

3 Press [ENTER] when prompted for a username.

4 Enter your password as requested (the default is “1234”).

5 Enter “bin” to set transfer mode to binary.

6 Use “put” to transfer files from the computer to the ZyXEL Device, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the ZyXEL Device and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the ZyXEL Device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the ZyXEL Device to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.

7 Enter “quit” to exit the ftp prompt.

29.5.4 FTP Session Example of Firmware File Upload

Figure 173   FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to Section 29.3.5 on page 244 to read about configurations that disallow TFTP and FTP over WAN.

29.5.5 TFTP File Upload

The ZyXEL Device also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1 Use telnet from your computer to connect to the ZyXEL Device and log in. Because TFTP does not have any security checks, the ZyXEL Device records the IP address of the telnet client and accepts TFTP requests only from this address.

2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

3 Enter the command “sys stdio 0” to disable the console timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute console timeout (default) when the file transfer is complete.

4 Launch the TFTP client on your computer and connect to the ZyXEL Device. Set the transfer mode to binary before starting data transfer.

5 Use the TFTP client (see the example below) to transfer files between the ZyXEL Device and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the ZyXEL Device in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyXEL Device to the computer, “put” the other way around, and “binary” to set binary transfer mode.

29.5.6 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyXEL Device’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyXEL Device).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

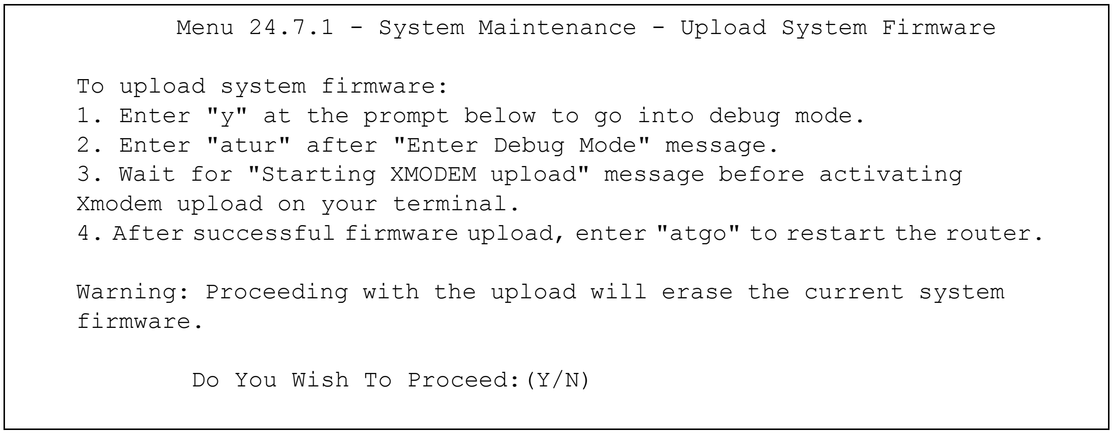
29.5.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your ZyXEL Device. However, in the event of your network being down, uploading files is only possible with a direct connection to your ZyXEL Device via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

29.5.8 Uploading Firmware File Via Console Port

1 Select 1 from Menu 24.7 – System Maintenance – Upload Firmware to display Menu 24.7.1 - System Maintenance - Upload System Firmware, and then follow the instructions as shown in the following screen.

Figure 174 Menu 24.7.1 As Seen Using the Console Port



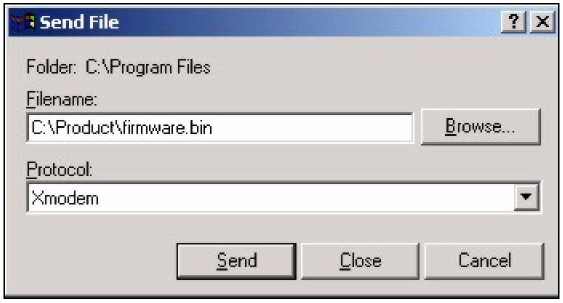
```
          Menu 24.7.1 - System Maintenance - Upload System Firmware

   To upload system firmware:
   1. Enter "y" at the prompt below to go into debug mode.
   2. Enter "atur" after "Enter Debug Mode" message.
   3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
   4. After successful firmware upload, enter "atgo" to restart the router.

   Warning: Proceeding with the upload will erase the current system
   firmware.

           Do You Wish To Proceed:(Y/N)
```

2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

29.5.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 175 Example Xmodem Upload



Folder: C:\Program Files

Filename: C:\Product\firmware.bin

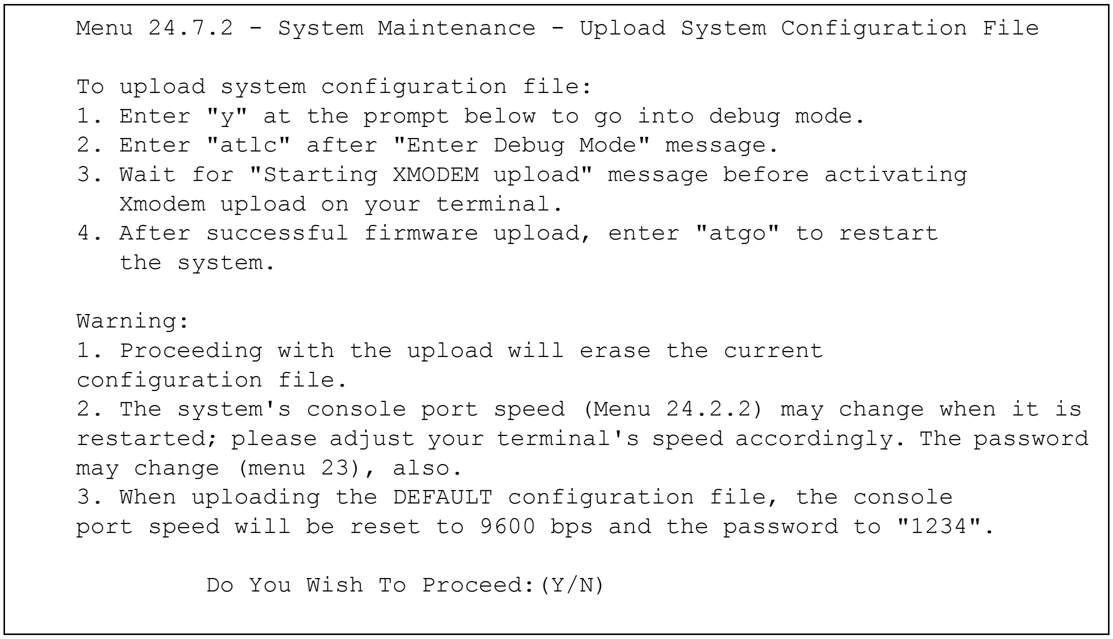
Protocol: Xmodem

After the firmware upload process has completed, the ZyXEL Device will automatically restart.

29.5.10 Uploading Configuration File Via Console Port

1 Select 2 from Menu 24.7 – System Maintenance – Upload Firmware to display Menu 24.7.2 - System Maintenance - Upload System Configuration File. Follow the instructions as shown in the next screen.

Figure 176 Menu 24.7.2 As Seen Using the Console Port



```
    Menu 24.7.2 - System Maintenance - Upload System Configuration File

    To upload system configuration file:
    1. Enter "y" at the prompt below to go into debug mode.
    2. Enter "atlc" after "Enter Debug Mode" message.
    3. Wait for "Starting XMODEM upload" message before activating
       Xmodem upload on your terminal.
    4. After successful firmware upload, enter "atgo" to restart
       the system.

    Warning:
    1. Proceeding with the upload will erase the current
    configuration file.
    2. The system's console port speed (Menu 24.2.2) may change when it is
    restarted; please adjust your terminal's speed accordingly. The password
    may change (menu 23), also.
    3. When uploading the DEFAULT configuration file, the console
    port speed will be reset to 9600 bps and the password to "1234".

             Do You Wish To Proceed:(Y/N)
```

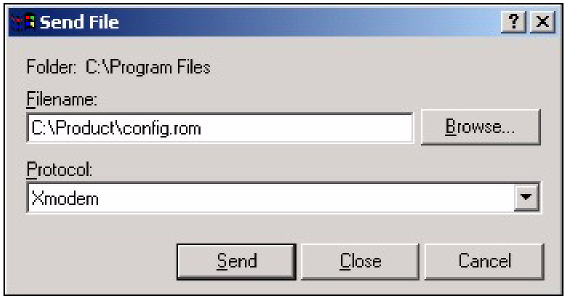
2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

3 Enter “atgo” to restart the ZyXEL Device.

29.5.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 177 Example Xmodem Upload



Folder: C:\Program Files

Filename: C:\Product\config.rom

Protocol: Xmodem

After the configuration upload process has completed, restart the ZyXEL Device by entering "atgo".

30

Menus 24.8 to 24.11

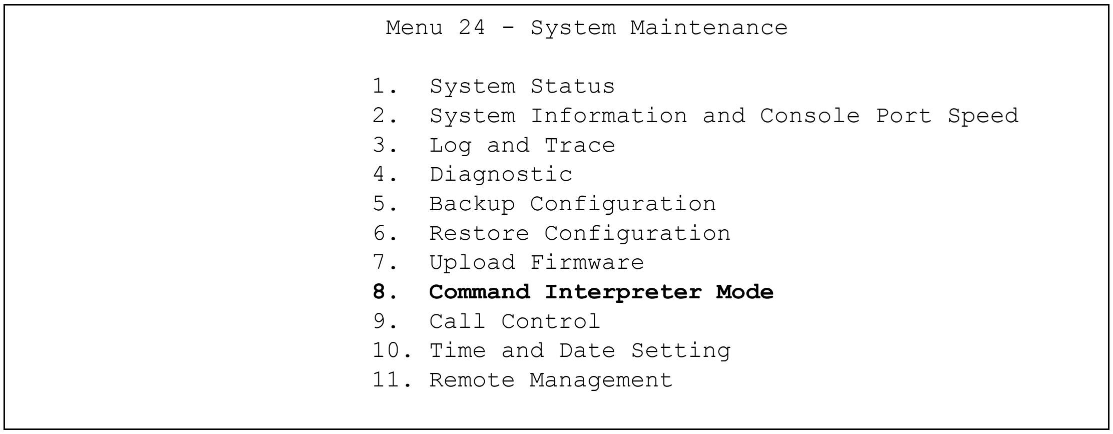
This chapter leads you through SMT menus 24.8 to 24.11.

30.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main router firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. Access can be by Telnet or by a connection to the console port, although some commands are only available with a console connection. See the included disk or zyxel.com for more detailed information on CI commands. Enter 8 from **Menu 24 - System Maintenance**.

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Figure 178 Command Mode in Menu 24



```
                              Menu 24 - System Maintenance

                             1.  System Status
                             2.  System Information and Console Port Speed
                             3.  Log and Trace
                             4.  Diagnostic
                             5.  Backup Configuration
                             6.  Restore Configuration
                             7.  Upload Firmware
                             8.  Command Interpreter Mode
                             9.  Call Control
                             10. Time and Date Setting
                             11. Remote Management
```

30.1.1 Command Syntax

The command keywords are in `courier new` font.

Enter the command keywords exactly as shown, do not abbreviate.

The required fields in a command are enclosed in angle brackets <>.

The optional fields in a command are enclosed in square brackets `[]`.

The `|` symbol means “or”.

For example,

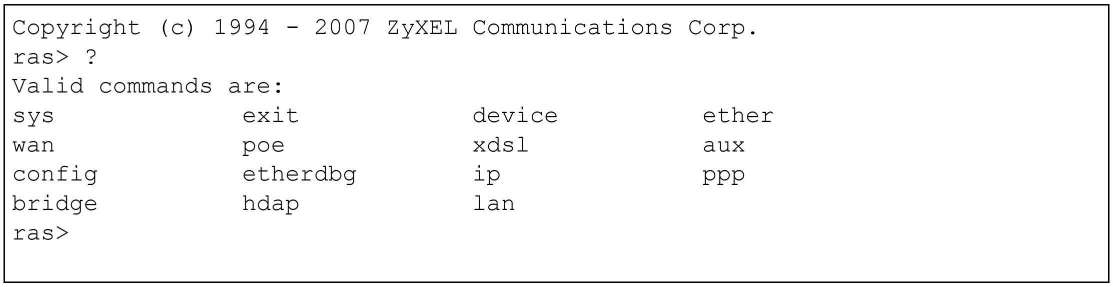
```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

30.1.2 Command Usage

A list of commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

Figure 179 Valid Commands



```
Copyright (c) 1994 - 2007 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
wan             poe             xdsl            aux
config          etherdbg        ip              ppp
bridge          hdap            lan
ras>
```

30.2 Call Control Support

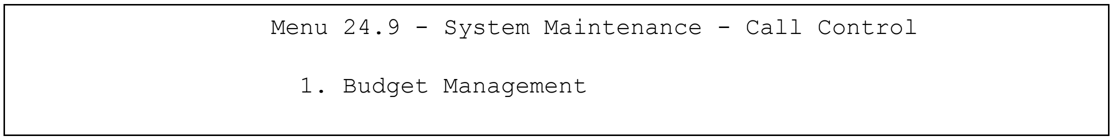
The ZyXEL Device provides a call control function for budget management. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPPoA** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the ZyXEL Device within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

Call history chronicles preceding incoming and outgoing calls.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 - System Maintenance - Call Control**, as shown in the next table.

Figure 180 Menu 24.9: System Maintenance - Call Control

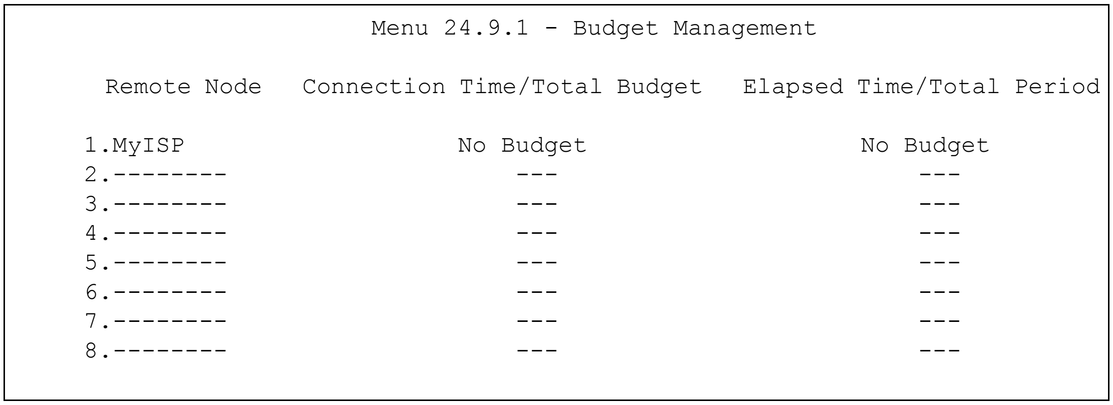


```
                  Menu 24.9 - System Maintenance - Call Control

                    1. Budget Management
```

30.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu. Not all fields are available on all models.

Figure 181 Menu 24.9.1 - Budget Management



```
                       Menu 24.9.1 - Budget Management

      Remote Node   Connection Time/Total Budget   Elapsed Time/Total Period

    1.MyISP                 No Budget                     No Budget
    2.--------                 ---                           ---
    3.--------                 ---                           ---
    4.--------                 ---                           ---
    5.--------                 ---                           ---
    6.--------                 ---                           ---
    7.--------                 ---                           ---
    8.--------                 ---                           ---
```

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

Table 88 Menu 24.9.1 - Budget Management

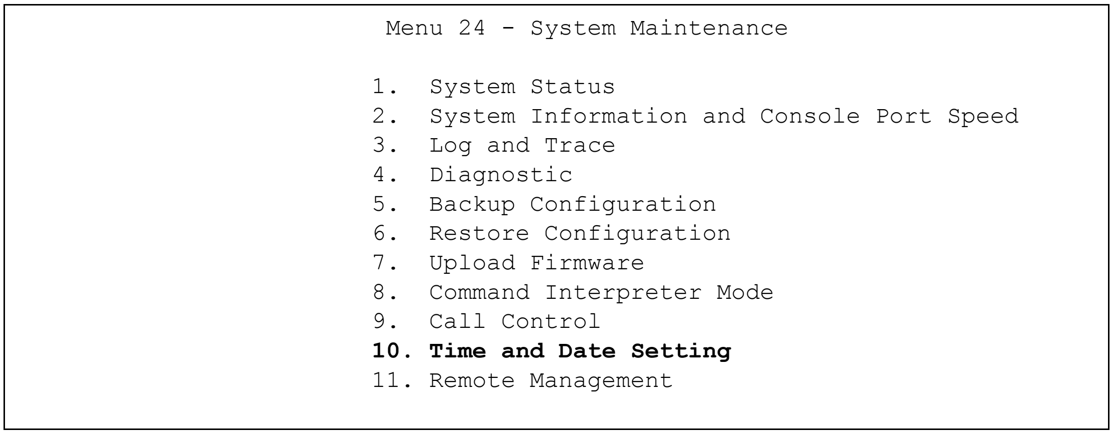
FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
Connection Time/ Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1).	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1-hour time period has lapsed.
Enter “0” to update the screen or press [ESC] to return to the previous screen.		

30.3 Time and Date Setting

The ZyXEL Device’s Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyXEL Device. Menu 24.10 allows you to update the time and date settings of your ZyXEL Device. The real time is then displayed in the ZyXEL Device error logs.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

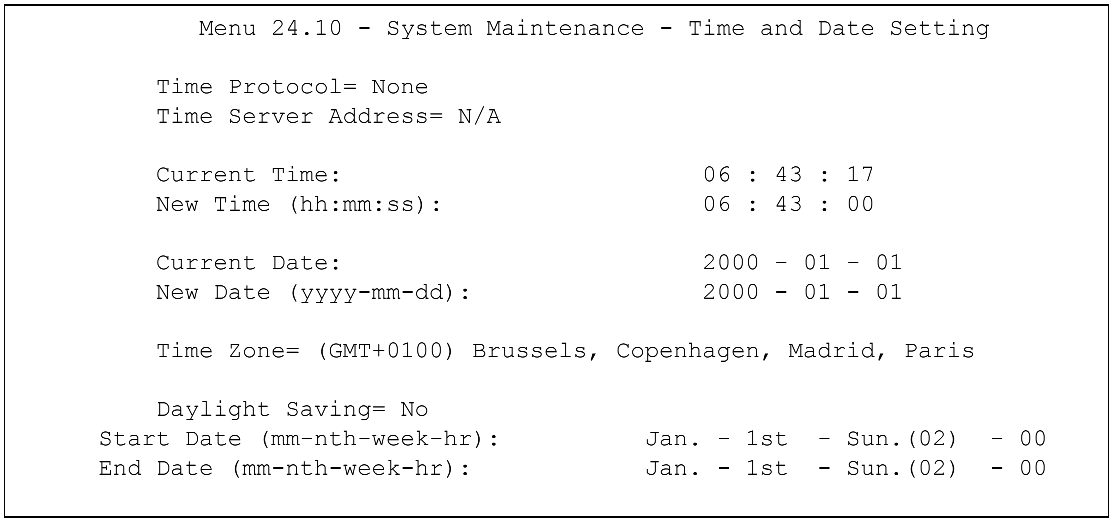
Figure 182 Menu 24: System Maintenance



```
                          Menu 24 - System Maintenance

                         1.  System Status
                         2.  System Information and Console Port Speed
                         3.  Log and Trace
                         4.  Diagnostic
                         5.  Backup Configuration
                         6.  Restore Configuration
                         7.  Upload Firmware
                         8.  Command Interpreter Mode
                         9.  Call Control
                         10. Time and Date Setting
                         11. Remote Management
```

Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your ZyXEL Device as shown in the following screen.

Figure 183 Menu 24.10: System Maintenance - Time and Date Setting



```
             Menu 24.10 - System Maintenance - Time and Date Setting

          Time Protocol= None
          Time Server Address= N/A

          Current Time:                        06 : 43 : 17
          New Time (hh:mm:ss):                 06 : 43 : 00

          Current Date:                        2000 - 01 - 01
          New Date (yyyy-mm-dd):               2000 - 01 - 01

          Time Zone= (GMT+0100) Brussels, Copenhagen, Madrid, Paris

          Daylight Saving= No
      Start Date (mm-nth-week-hr):          Jan. - 1st  - Sun.(02)  - 00
      End Date (mm-nth-week-hr):            Jan. - 1st  - Sun.(02)  - 00
```

The following table describes the fields in this screen.

Table 89 Menu 24.10: System Maintenance - Time and Date Setting

FIELD	DESCRIPTION
Use Time Server When Bootup	Press [SPACE BAR] and then enter the time service protocol that your timeserver uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, **NTP (RFC-1305)**, is similar to **Time (RFC-868)**. Select **None** to enter the new time and new date manually.
Time Server Address	Enter the IP address or domain name of your timeserver. Check with your ISP/ network administrator if you are unsure of this information. The default is tick.stdtime.gov.tw

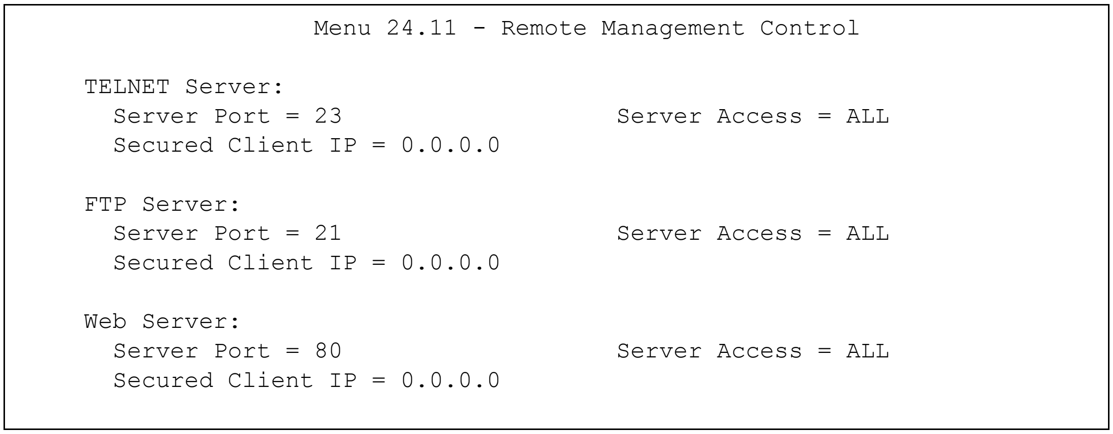
Table 89 Menu 24.10: System Maintenance - Time and Date Setting (continued)

FIELD	DESCRIPTION
Current Time	This field displays an updated time only when you reenter this menu.
New Time (hh:mm:ss)	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you reenter this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daylight time in the evenings. If you use daylight savings time, then choose **Yes**.
Start Date (mm-dd)	Configure the day and time when Daylight Saving Time starts if you selected **Yes** in the **Daylight Saving** field. The **hr** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and **2:00**. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Mar.**, **Last**, **Sun.** The time you type in the **hr** field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date (mm-dd)	Configure the day and time when Daylight Saving Time ends if you selected **Yes** in the **Daylight Saving** field. The **hr** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and **2:00**. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Oct.**, **Last**, **Sun.** The time you type in the **hr** field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Once you have filled in this menu, press [ENTER] at the message “Press ENTER to Confirm or ESC to Cancel“ to save your configuration, or press [ESC] to cancel.	

30.4 Remote Management

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field. Enter 11 from menu 24 to bring up **Menu 24.11 - Remote Management Control**.

Figure 184 Menu 24.11 – Remote Management Control



```
                    Menu 24.11 - Remote Management Control

     TELNET Server:
       Server Port = 23                   Server Access = ALL
       Secured Client IP = 0.0.0.0

     FTP Server:
       Server Port = 21                   Server Access = ALL
       Secured Client IP = 0.0.0.0

     Web Server:
       Server Port = 80                   Server Access = ALL
       Secured Client IP = 0.0.0.0
```

The following table describes the fields in this screen.

Table 90 Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION
TELNET Server FTP Server Web Server	Each of these read-only labels denotes a service that you may use to remotely manage the ZyXEL Device.
Server Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the ZyXEL Device.
Server Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: **LAN only**, **WAN only**, **ALL** or **Disable**.
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the ZyXEL Device. Enter an IP address to restrict access to a client with a matching IP address.
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

30.4.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secure Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

31

IP Routing Policy Setup

Use this menu to look at and configure policy routes.

31.1 Policy Route

Traditionally, routing is based on the destination address only and the ZyXEL Device takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

31.2 Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Bandwidth Shaping – Organizations can allocate bandwidth to traffic that matches the routing policy and prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.
- NAT - The ZyXEL Device performs NAT by default for traffic going to or from the **ge1** interface. Routing policy's SNAT allows network administrators to have traffic received on a specified interface use a specified IP address as the source IP address.

31.3 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria can include the user name, source address and incoming interface, destination address, schedule, IP protocol (ICMP, UDP, TCP, etc.) and port.

The actions that can be taken include:

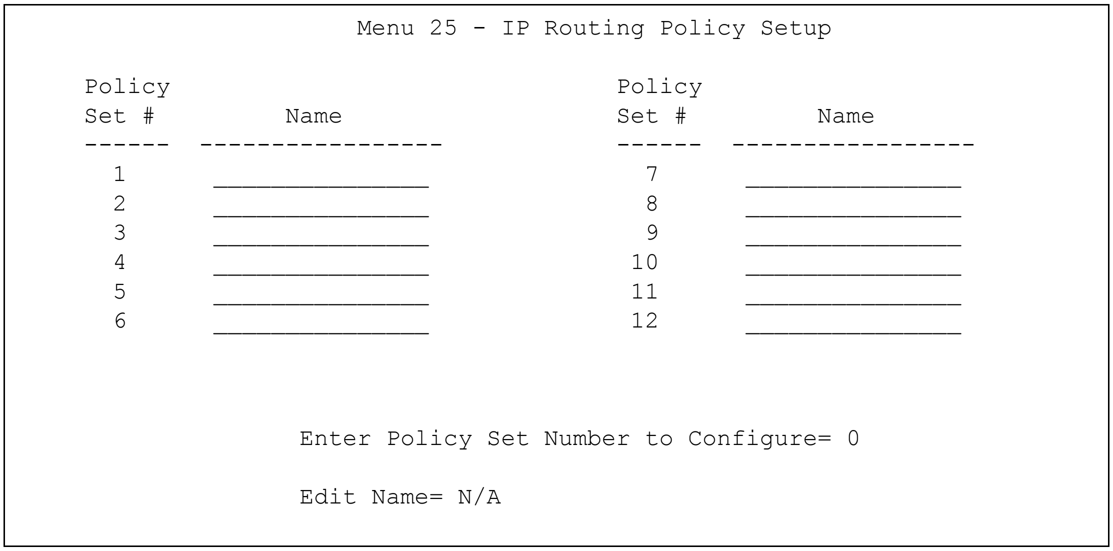
- Routing the packet to a different gateway, outgoing interface, or trunk.
- Limiting the amount of bandwidth available and setting a priority for traffic.

IPPR follows the existing packet filtering facility of RAS in style and in implementation.

31.4 IP Routing Policy Setup

Use this menu to look at a summary of policy routes. To open this menu, enter 25 in the main menu.

Figure 185 Menu 25: IP Routing Policy Setup



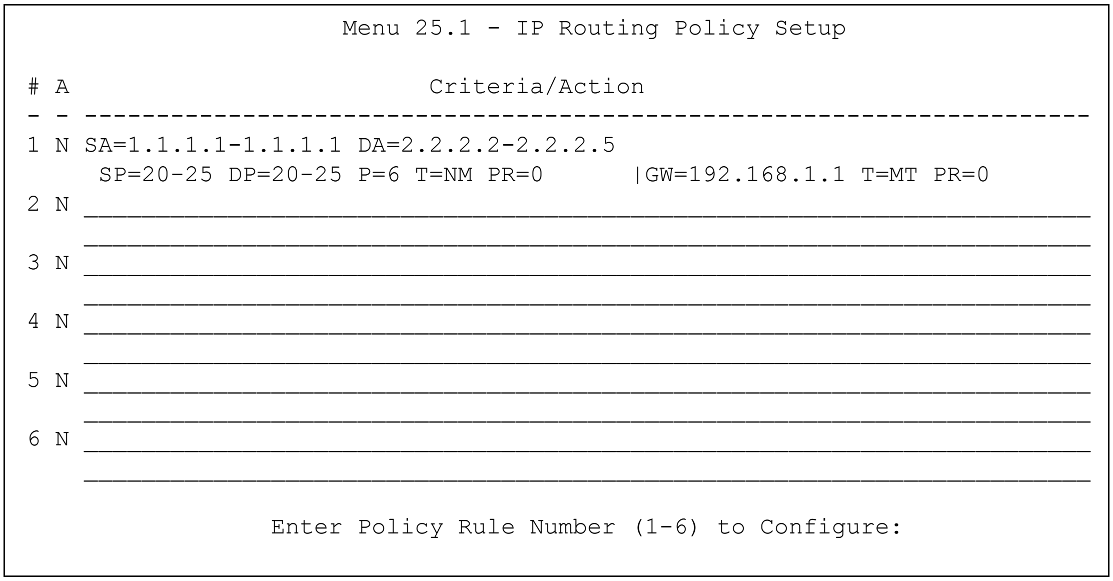
```
                        Menu 25 - IP Routing Policy Setup

     Policy                                     Policy
     Set #         Name                         Set #         Name
     ------  -----------------                  ------  -----------------
       1      _______________                     7      _______________
       2      _______________                     8      _______________
       3      _______________                     9      _______________
       4      _______________                    10      _______________
       5      _______________                    11      _______________
       6      _______________                    12      _______________



                    Enter Policy Set Number to Configure= 0

                    Edit Name= N/A
```

1. Select the filter set you wish to configure (1-12) and press [ENTER].
2. Enter a descriptive name or comment in the **Edit Name** field and press [ENTER].
3. Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 25.1 - IP Routing Policy Setup**.

31.5 IP Routing Policy Setup

Use this menu to look at a policy route. To open this menu, enter the number and name of a policy route in menu 25.

Figure 186 Menu 25.1: IP Routing Policy Setup



```
                      Menu 25.1 - IP Routing Policy Setup

# A                            Criteria/Action
- - ----------------------------------------------------------------------
1 N SA=1.1.1.1-1.1.1.1 DA=2.2.2.2-2.2.2.5
     SP=20-25 DP=20-25 P=6 T=NM PR=0      |GW=192.168.1.1 T=MT PR=0
2 N ______________________________________________________________________
    ______________________________________________________________________
3 N ______________________________________________________________________
    ______________________________________________________________________
4 N ______________________________________________________________________
    ______________________________________________________________________
5 N ______________________________________________________________________
    ______________________________________________________________________
6 N ______________________________________________________________________
    ______________________________________________________________________

                 Enter Policy Rule Number (1-6) to Configure:
```

The following table describes the labels in this menu.

Table 91 Menu 25.1: IP Routing Policy Setup

FIELD	DESCRIPTION
#	This field displays the rule number.
Criteria/Action	See Table 92 on page 263.
Enter Policy Rule Number (1-6) to Configure	Enter the rule number you would like to edit.

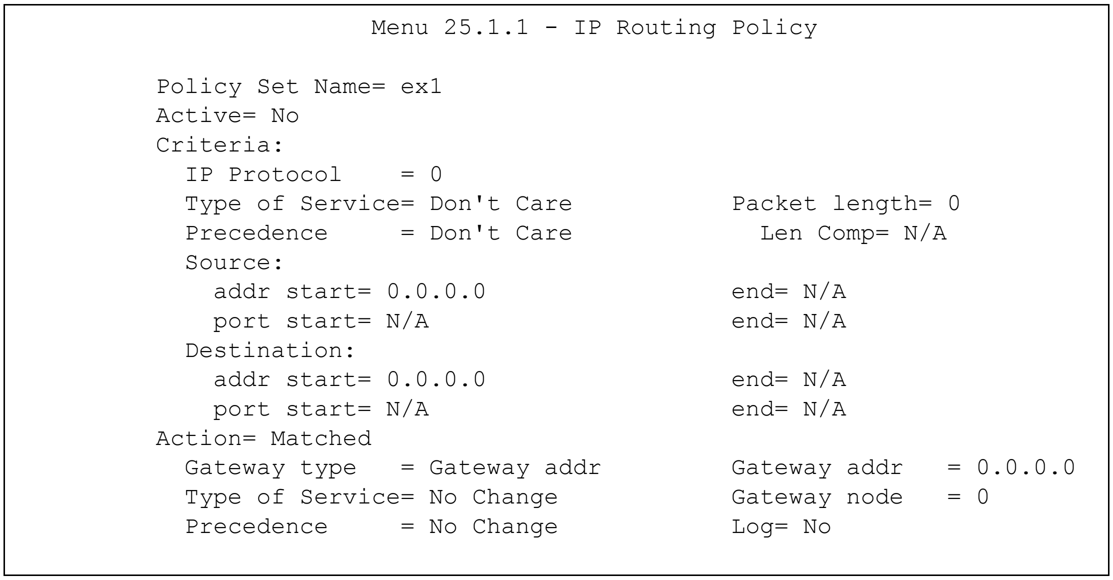
Table 92 Menu 25: IP Routing Policy Setup, Abbreviations

ABBREVIATION		MEANING
	SA	Source IP Address
	SP	Source Port
	DA	Destination IP Address
	DP	Destination Port
	P	IP layer 4 protocol number (TCP=6, UDP=17…)
	T	Type of service of incoming packet
	PR	Precedence of incoming packet
Action	GW	Gateway IP address
	T	Outgoing Type of service
	P	Outgoing Precedence
Service	NM	Normal
	MD	Minimum Delay
	MT	Maximum Throughput
	MR	Maximum Reliability
	MC	Minimum Cost

31.6 IP Routing Policy

Use this menu to configure policy routes. To open this menu, select **Edit** and enter the appropriate rule number in menu 25.

Figure 187 Menu 25.1.1: IP Routing Policy



```
                        Menu 25.1.1 - IP Routing Policy

          Policy Set Name= ex1
          Active= No
          Criteria:
            IP Protocol    = 0
            Type of Service= Don't Care           Packet length= 0
            Precedence     = Don't Care             Len Comp= N/A
            Source:
              addr start= 0.0.0.0                 end= N/A
              port start= N/A                     end= N/A
            Destination:
              addr start= 0.0.0.0                 end= N/A
              port start= N/A                     end= N/A
          Action= Matched
            Gateway type   = Gateway addr         Gateway addr   = 0.0.0.0
            Type of Service= No Change            Gateway node   = 0
            Precedence     = No Change            Log= No
```

The following table describes the labels in this menu.

Table 93 Menu 25.1.1: IP Routing Policy

FIELD	DESCRIPTION
Policy Set Name	This is the descriptive name of the routing policy selected in **Menu 25.1 - IP Routing Policy Summary**.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the policy.
Criteria	
IP Protocol	Enter a number that represents an IP layer 4 protocol, for example, UDP=17, TCP=6, ICMP=1 and Don't care=0.
Type of Service	Prioritize incoming network traffic by choosing from **Don't Care**, **Normal**, **Min Delay**, **Max Thruput** or **Max Reliable**.
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from **0** to **7** or **Don't Care**.
Packet Length	Type the length of incoming packets (in bytes). The operators in the **Len Comp** (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**.
Source	
addr start / end	Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination	
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.

Table 93 Menu 25.1.1: IP Routing Policy (continued)

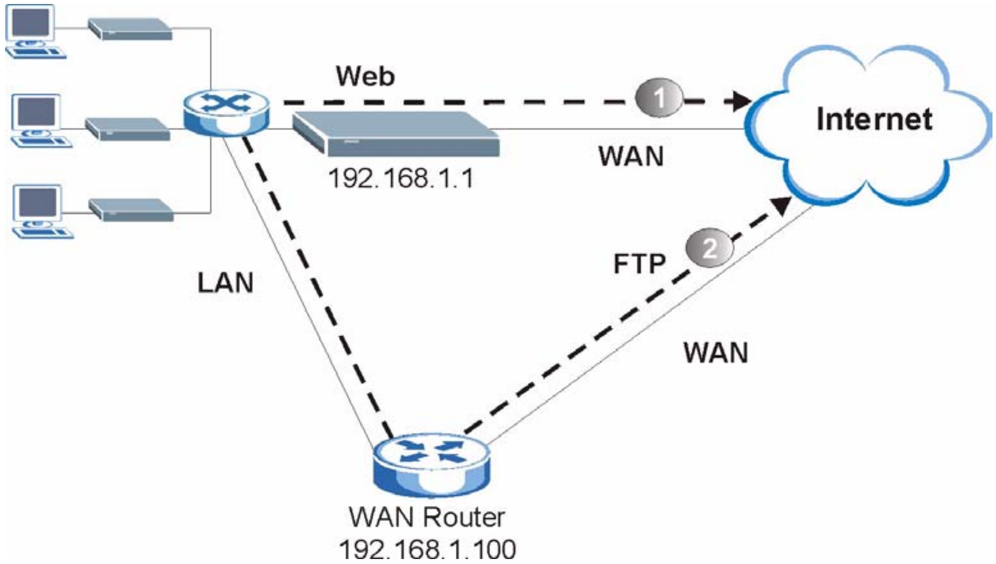
FIELD	DESCRIPTION
Action	Specifies whether action should be taken on criteria Matched or Not Matched.
Gateway type	Press [SPACE BAR] and then [ENTER] to select **Gateway addr** and enter the IP address of the gateway if you want to specify the IP address of the gateway. The gateway is an immediate neighbor of your ZyXEL Device that will forward the packet to the destination. The gateway must be a router on the same segment as your ZyXEL Device's LAN or WAN port. Press [SPACE BAR] and then [ENTER] to select **Gateway node** to enter the remote node number of the gateway if you want to have the ZyXEL Device send traffic that matches the policy route through a specific WAN port.
Gateway addr	If you selected **Gateway addr** in the **Gateway type** field, enter the IP address of the gateway to which the ZyXEL Device forwards the packet. The gateway is an immediate neighbor of your ZyXEL Device and must be on the same subnet as the ZyXEL Device, if it is on the LAN, or the IP address of a remote node, if it is on the WAN. Enter 0.0.0.0 to specify the default gateway.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **No Change**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**.
Gateway node	If you selected **Gateway node** in the **Gateway type** field, enter the remote node number (one to eight) of the gateway to which the ZyXEL Device forwards the packet. A remote node represents both the remote gateway and the network behind it across a WAN connection. For more information of how to set up a remote node profile, see Menu 11: Remote Node Setup in Section 22.2 on page 185.
Precedence	Set the new outgoing packet precedence value. Values are **0** to **7** or **Don't Care**.
Log	Press [SPACE BAR] and then [ENTER] to select **Yes** to make an entry in the system log when a policy is executed.

31.7 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

Route 1 represents the default IP route and route 2 represents the configured IP route.

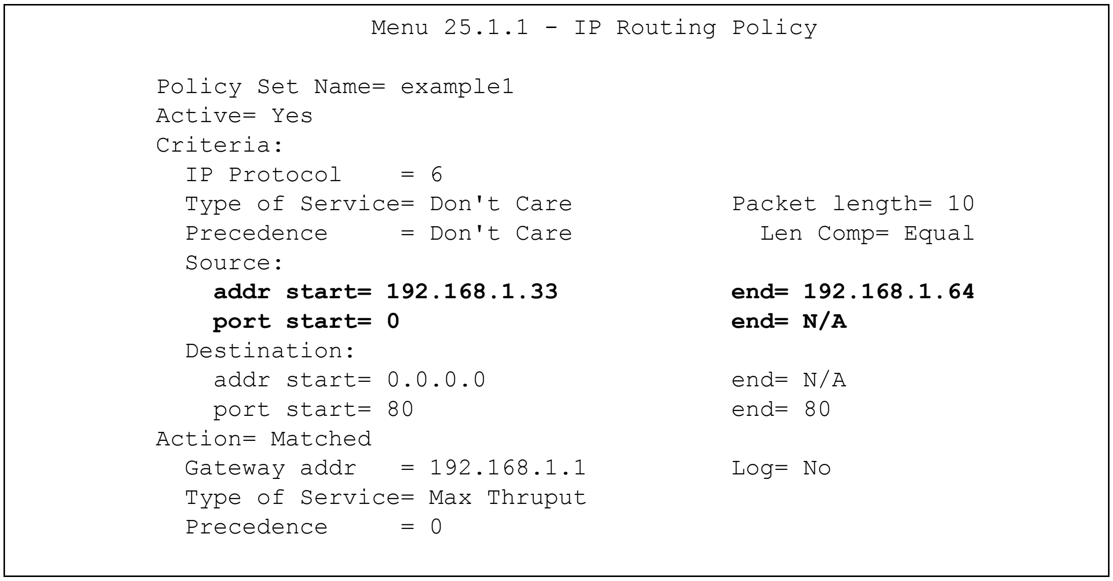
Figure 188 IP Routing Policy Example



To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the ZyWALL, follow the steps as shown next.

1 Create a rule in **Menu 25.1 - IP Routing Policy Setup** as shown next.

Figure 189 IP Routing Policy Example 1



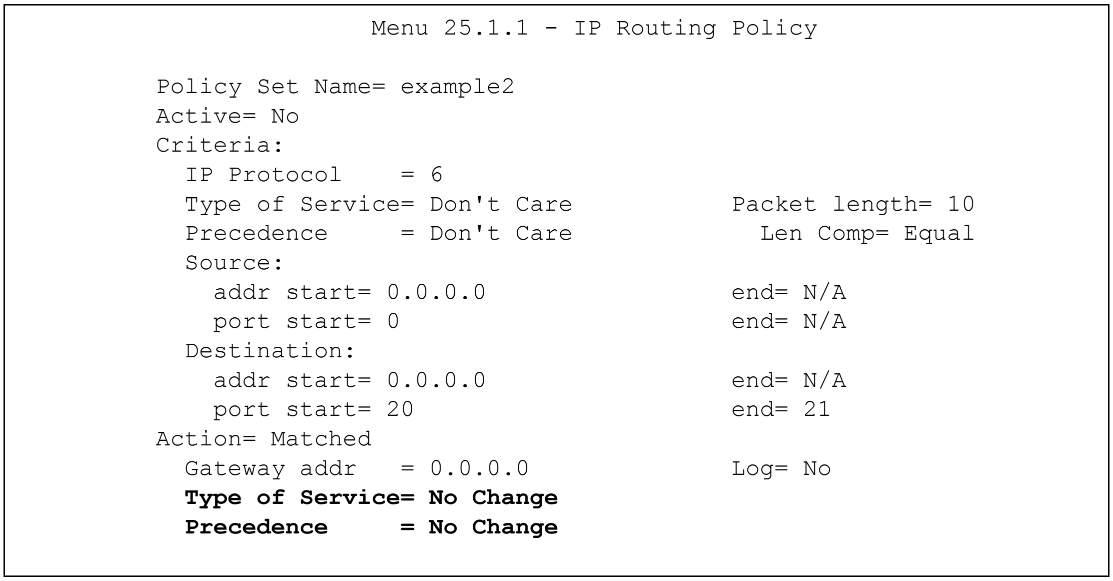
```
                      Menu 25.1.1 - IP Routing Policy

          Policy Set Name= example1
          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Don't Care          Packet length= 10
            Precedence     = Don't Care            Len Comp= Equal
            Source:
              addr start= 192.168.1.33           end= 192.168.1.64
              port start= 0                      end= N/A
            Destination:
              addr start= 0.0.0.0                end= N/A
              port start= 80                     end= 80
          Action= Matched
            Gateway addr   = 192.168.1.1         Log= No
            Type of Service= Max Thruput
            Precedence     = 0
```

2 Select **Yes** in the **LAN** field in menu 25.1.1 to apply the policy to packets received on the LAN port.

3 Check **Menu 25 - IP Routing Policy Summary** to see if the rule is added correctly.

4 Create another rule in menu 25.1 for this rule to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

Figure 190 IP Routing Policy Example 2



```
                    Menu 25.1.1 - IP Routing Policy

          Policy Set Name= example2
          Active= No
          Criteria:
            IP Protocol    = 6
            Type of Service= Don't Care           Packet length= 10
            Precedence     = Don't Care             Len Comp= Equal
            Source:
              addr start= 0.0.0.0                 end= N/A
              port start= 0                       end= N/A
            Destination:
              addr start= 0.0.0.0                 end= N/A
              port start= 20                      end= 21
          Action= Matched
            Gateway addr   = 0.0.0.0              Log= No
            Type of Service= No Change
            Precedence     = No Change
```

5 Check **Menu 25 - IP Routing Policy Summary** to see if the rule is added correctly.

32

Schedule Setup

Use this menu to look at and configure the schedule sets in the ZyXEL Device.

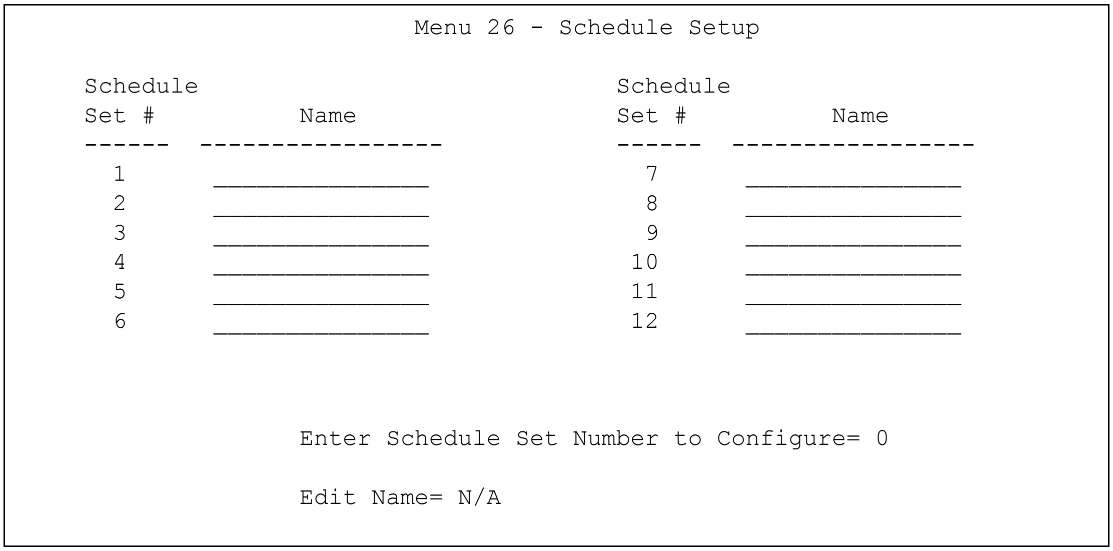
32.1 Schedule Set Overview

Call scheduling (applicable for PPPoE encapsulation only) allows the ZyXEL Device to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler that lets you specify a time period to record a television program in a VCR or TiVo.

32.2 Schedule Setup

This menu is only applicable if your Internet connection uses PPPoE encapsulation. Use this menu to look at the schedule sets in the ZyXEL Device. To open this menu, enter 26 in the main menu.

Figure 191 Menu 26: Schedule Setup



```
                           Menu 26 - Schedule Setup

    Schedule                             Schedule
    Set #          Name                  Set #          Name
    ------  -----------------            ------  -----------------
      1      _______________               7      _______________
      2      _______________               8      _______________
      3      _______________               9      _______________
      4      _______________              10      _______________
      5      _______________              11      _______________
      6      _______________              12      _______________


                   Enter Schedule Set Number to Configure= 0

                   Edit Name= N/A
```

The following table describes the labels in this menu.

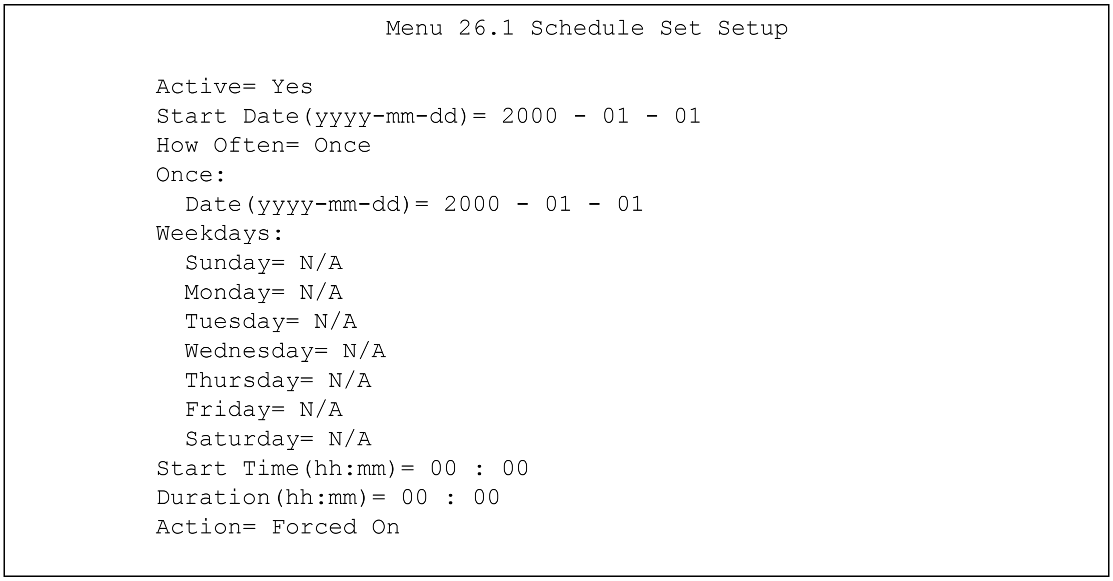
Table 94 Menu 26: Schedule Setup

FIELD	DESCRIPTION
1-12	This field shows the beginning of the name of each schedule set. Lower numbered sets take precedence over higher numbered sets. This avoids scheduling conflicts. For example, if sets 1, 2, 3 and 4 in are applied in the remote node, then set 1 takes precedence over set 2, 3 and 4.
Enter Schedule Set Number to Configure	If you want to configure a schedule set, enter the number of the static route in this field, enter the name in the **Edit Name** field, and press [ENTER]. Menu 26.1 appears. If you want to delete a schedule set, enter the number of the static route in this field, leave the name blank in the **Edit Name** field, and press [ENTER].
Edit Name	Enter the name of the schedule set you want to configure, or leave this field blank to delete the specified schedule set.

32.3 Schedule Set Setup

This menu is only applicable if your Internet connection uses PPPoE encapsulation. Use this menu to configure the schedule sets in the ZyXEL Device. To open this menu, enter the number of the schedule set in the **Enter Schedule Set Number to Configure** field, enter the name of the schedule set in the **Edit Name** field, and press [ENTER] in menu 26.

Figure 192 Menu 26.1: Schedule Set Setup



```
                         Menu 26.1 Schedule Set Setup

         Active= Yes
         Start Date(yyyy-mm-dd)= 2000 - 01 - 01
         How Often= Once
         Once:
           Date(yyyy-mm-dd)= 2000 - 01 - 01
         Weekdays:
           Sunday= N/A
           Monday= N/A
           Tuesday= N/A
           Wednesday= N/A
           Thursday= N/A
           Friday= N/A
           Saturday= N/A
         Start Time(hh:mm)= 00 : 00
         Duration(hh:mm)= 00 : 00
         Action= Forced On
```

The following table describes the labels in this menu.

Table 95 Menu 26.1: Schedule Set Setup

FIELD	DESCRIPTION
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.
Start Date	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.
How Often	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.
Once	
Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.
Weekdays	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.

33

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyXEL Device Access and Login
- Internet Access

33.1 Power, Hardware Connections, and LEDs

? The ZyXEL Device does not turn on. None of the LEDs turn on.

1 Make sure the ZyXEL Device is turned on.

2 Make sure you are using the power adaptor or cord included with the ZyXEL Device.

3 Make sure the power adaptor or cord is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.

4 Turn the ZyXEL Device off and on.

5 If the problem continues, contact the vendor.

? One of the LEDs does not behave as expected.

1 Make sure you understand the normal behavior of the LED. See Section 1.4 on page 35.

2 Check the hardware connections. See the Quick Start Guide.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Turn the ZyXEL Device off and on.

5 If the problem continues, contact the vendor.

33.2 ZyXEL Device Access and Login

I forgot the IP address for the ZyXEL Device.

1 The default IP address is **192.168.1.1**.

2 Use the console port to log in to the ZyXEL Device. (has external console port)

3 If you changed the IP address and have forgotten it, you might get the IP address of the ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start** > **Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.

4 If this does not work, you have to reset the device to its factory defaults. See Section 33.4 on page 277.

I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 33.4 on page 277.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address (Section 6.3 on page 87), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the ZyXEL Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 33.1 on page 273.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix C on page 303.

4 Make sure your computer is in the same subnet as the ZyXEL Device. (If you know that there are routers between your computer and the ZyXEL Device, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Appendix B on page 287. Your ZyXEL Device is a DHCP server by default.

5 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See Section 33.4 on page 277.

6 If the problem continues, contact the network administrator or vendor, or try the advanced suggestion.

Advanced Suggestion

- Try to access the ZyXEL Device using another service, such as Telnet. If you can access the ZyXEL Device, check the remote management settings and SMT filters to find out why the ZyXEL Device does not respond to HTTP. See Section 17.2 on page 163.

I can see the **Login** screen, but I cannot log in to the ZyXEL Device.

1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using the SMT, Telnet, or the console port to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.

3 Turn the ZyXEL Device off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 33.4 on page 277.

I cannot access the SMT. I cannot Telnet to the ZyXEL Device.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use the console port to access the ZyXEL Device.

Make sure that you are using the included console cable and that the **CON/AUX** switch on the ZyXEL Device is set to **CON**. See the Quick Start Guide.

33.3 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.4 on page 35.

2 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.4 on page 35.

2 Turn the ZyXEL Device off and on.

3 If the problem continues, contact your ISP. (

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.4 on page 35. If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Turn the ZyXEL Device and your computer off and on.

3 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

I cannot access a website.

Check your content filtering settings and make sure you do not block yourself access to any websites. See Chapter 10 on page 149.

My dial backup or traffic redirect do not work.

1 If you are using the **CON/AUX** port for your dial backup, make sure that the **CON/AUX** switch on the ZyXEL Device is set to **AUX**. See the Quick Start Guide.

2 If you are using a point-to-2point configuration, WAN backup is disabled.

33.4 Reset the ZyXEL Device to Its Factory Defaults

If you reset the ZyXEL Device, you lose all of the changes you have made. The ZyXEL Device re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

? You will lose all of your changes when you push the **RESET** button.

To reset the ZyXEL Device,

1 Make sure the **POWER LED** is on and not blinking.

2 Press and hold the **RESET** button for ten seconds. Release the **RESET** button when the **POWER** LED begins to blink. The default settings have been restored.

If the ZyXEL Device restarts automatically, wait for the ZyXEL Device to finish restarting, and log in to the web configurator. The password is “1234”.

If the ZyXEL Device does not restart automatically, disconnect and reconnect the ZyXEL Device’s power. Then, follow the directions above again.

PART VII
Appendices and Index

A

Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

Table 96 Hardware Specifications

SPECIFICATION	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	user: "user" administrator: "1234"
DHCP Pool	192.168.1.33 to 192.168.1.64
Dimensions (W x D x H)	180 x 127 x 36 mm
Power Specification	AC version: 9V AC 1A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
G.SHDSL Port	RJ-11 interface Data Rate: 192 Kbps - 5700 Kbps Line Code: TC-PAM modulation Line Impedance: 135 W Connection Loops: one pair (2-wire)
Operating Environment	Temperature: 0º C ~ 40º C Humidity: 20% ~ 90% RH (non-condensing)
Storage Environment	Temperature: -20º C ~ 60º C Humidity: 20% ~ 90% RH
Distance between the centers of the holes on the device's back.	108 mm
Screw size for wall-mounting	M4 Tap Screw, see Figure 194 on page 285.

Table 97 Firmware

Routing/Bridge Support	IP (RFC 791) routing is supported. TCP, UDP, ICMP, IGMP v1 and v2, ARP, RIP v1, RIP v2 Transparent bridging (IEEE 802.1D) PPP BCP (RFC 3185) support
G.SHDSL	TC-PAM line modulation Configurable as either server or client mode Rate negotiating / Manually rate adaptation configuration

Table 97 Firmware (continued)

ATM Support	Multiple protocols over AAL5 (RFC1483) PPP over ATM (RFC 2364) PPP over Ethernet (RFC2516) ATM AAL5 supported Support 8 PVCs ATM Forum UNI3.0/4.0 PVC OAM F4/F5 Loopback, RDI, AIS UBR CBR, and nrt-VBR traffic shaping
Internet Access Sharing	NAT (includes multi-to-multi NAT) / SUA, 2048 NAT sessions Port restricted cone NAT NAT server (Port forwarding) Multi-NAT Dynamic DNS (www.dyndns.org) DHCP server/client/relay
Security	Packet Filtering User Authentication (PAP, CHAP) with PPP (RFC 1334, RFC 1994) Microsoft CHAP
Network Management	Web-based Configuration Command-line interface Password-protected Telnet support SNMP MIB I /MIB II support TFTP & FTP firmware upgrade and configuration backup
Diagnostics Capabilities (for the following circuitry)	FLASH memory SDSL circuitry RAM LAN port
Others	DNS Proxy UNIX syslog

Table 98 Firmware Features

FEATURE	DESCRIPTION
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the ZyXEL Device. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the ZyXEL Device’s configuration. You can put it back on the ZyXEL Device later if you decide to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.
Packet Filters	The ZyXEL Device's packet filtering functions allows added network security and management.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network.

Table 98 Firmware Features

FEATURE	DESCRIPTION
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
IP Alias	IP alias allows you to subdivide a physical network into logical networks over the same Ethernet interface with the ZyXEL Device itself as the gateway for each subnet.
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. You can also set the time manually. These dates and times are then used in logs.
Logging and Tracing	Use packet tracing and logs for troubleshooting. You can send logs from the ZyXEL Device to an external syslog server.
PPPoE	PPPoE mimics a dial-up Internet access connection.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the ZyXEL Device.

Table 99 Standards Supported

STANDARD	DESCRIPTION
RFC 1483/2684 (MPOA)	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2364 (PPPoA)	PPP over AAL5
RFC 2516 (PPPoE)	PPP over Ethernet
ITU G.991.2 (G.SHDSL/ G.SHDSL.bis)	ITU standard for Single-pair high-speed digital subscriber line (SHDSL) transceivers
RFC 1112 (IGMP v1)	Internet Group Management Protocol, Version 1
RFC 2236 (IGMP v2)	Internet Group Management Protocol, Version 2
RFC 867	Daytime Protocol
RFC 868	Time Protocol
RFC 1305	Network Time Protocol (Version 3) Specification, Implementation
RFC 1334 (PAP)	PPP Authentication Protocols
RFC 1994 (CHAP)	PPP Challenge Handshake Authentication Protocol
RFC 1332 (IPCP)	The PPP Internet Protocol Control Protocol
RFC 1058 (RIP-1)	Routing Information Protocol
RFC 1723 (RIP-2)	RIP Version 2 - Carrying Additional Information
RFC 1631 (NAT)	IP Network Address Translator
RFC 1661 (PPP)	The Point-to-Point Protocol
RFC 1157 (SNMPv1)	Simple Network Management Protocol, Version 1
RFC 1441 (SNMPv2)	Simple Network Management Protocol, Version 2

Wall-mounting Instructions

Complete the following steps to hang your ZyXEL Device on a wall.

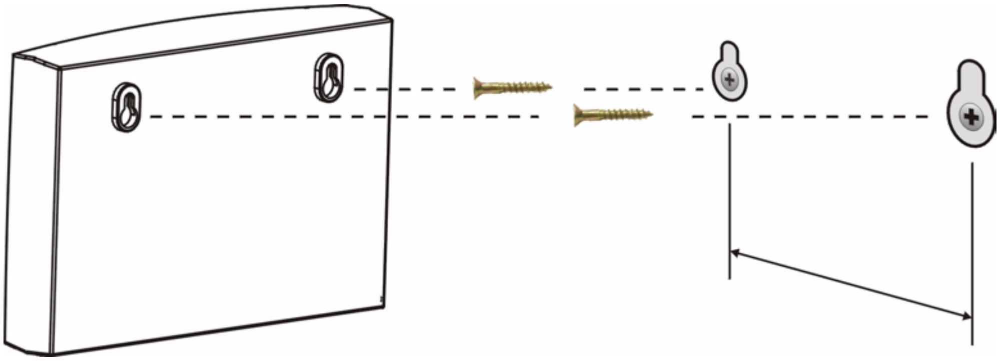
See Table 96 on page 281 for the size of screws to use and how far apart to place them.

1. Select a position free of obstructions on a sturdy wall.
2. Drill two holes for the screws.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

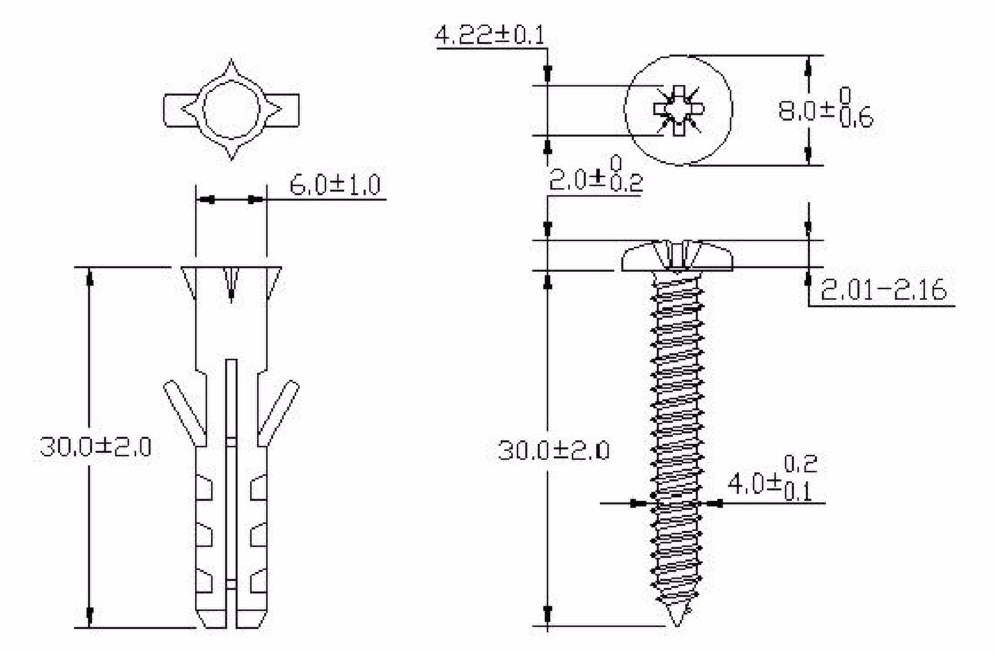
3. Do not insert the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.
4. Make sure the screws are snugly fastened to the wall. They need to hold the weight of the ZyXEL Device with the connection cables.
5. Align the holes on the back of the ZyXEL Device with the screws on the wall. Hang the ZyXEL Device on the screws.

Figure 193 Wall-mounting Example



The following are dimensions of an M4 tap screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

Figure 194 Masonry Plug and M4 Tap Screw



Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

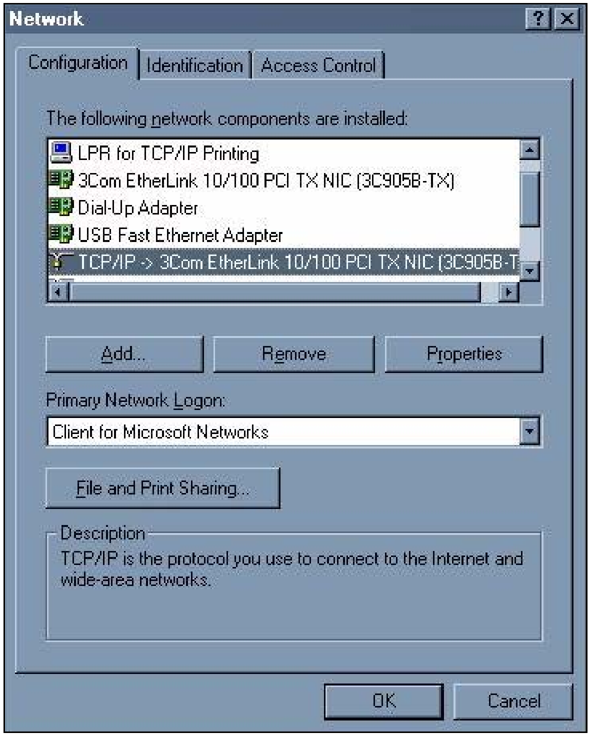
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyXEL Device's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 195 WIndows 95/98/Me: Network: Configuration



The following network components are installed:

LPR for TCP/IP Printing
3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
Dial-Up Adapter
USB Fast Ethernet Adapter
TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T

Primary Network Logon:
Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.
3. Select **Microsoft** from the list of manufacturers.
4. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
5. Restart your computer so the changes you made take effect.

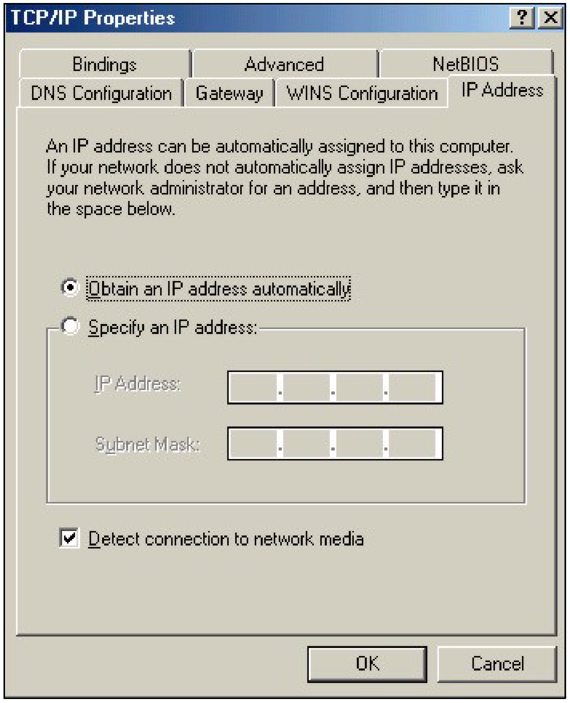
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 196 Windows 95/98/Me: TCP/IP Properties: IP Address



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

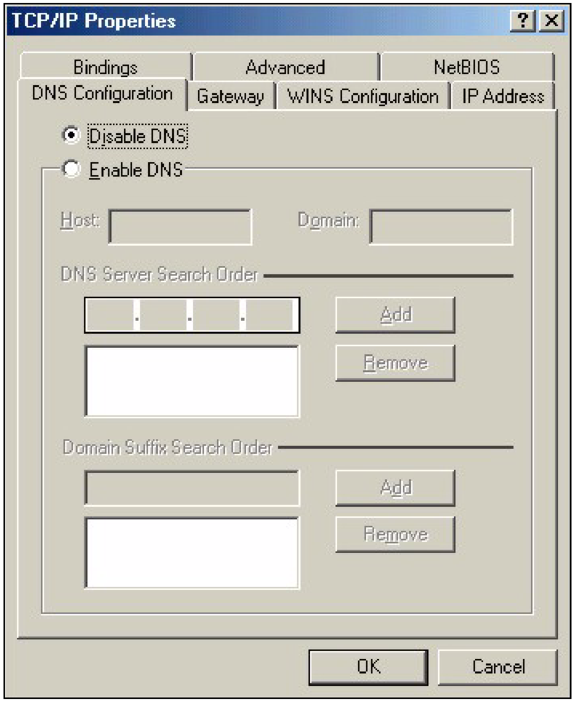
Subnet Mask: . . .

☑ Detect connection to network media

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 197 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



● Disable DNS

○ Enable DNS

4 Click the **Gateway** tab.

- If you do not know your gateway’s IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your ZyXEL Device and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

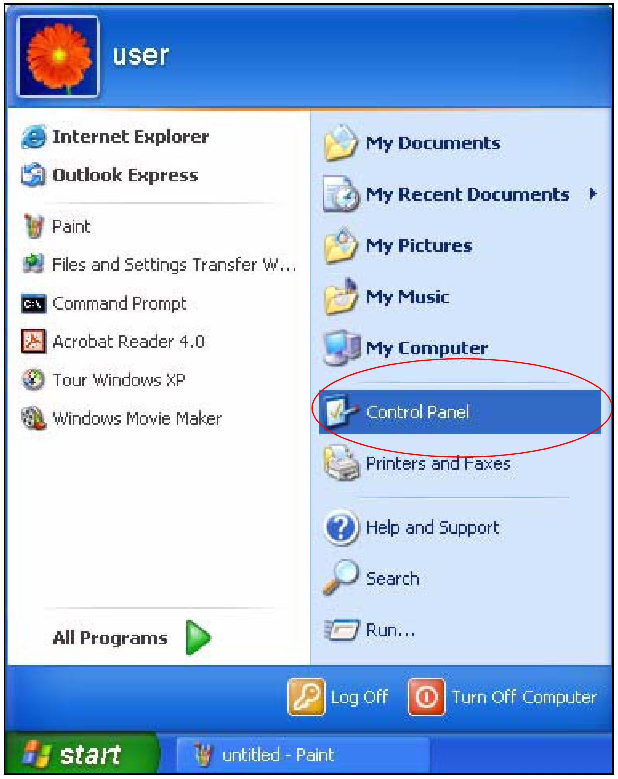
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

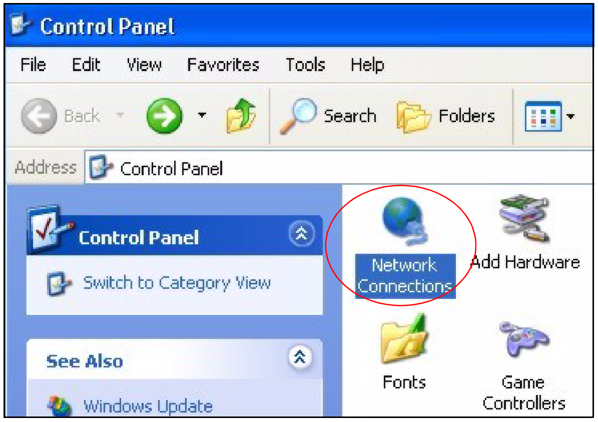
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 198 Windows XP: Start Menu



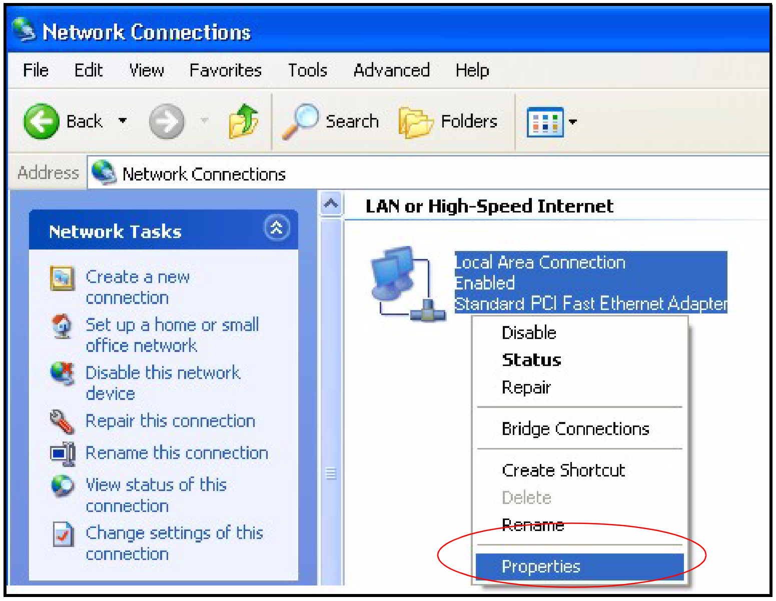
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 199 Windows XP: Control Panel



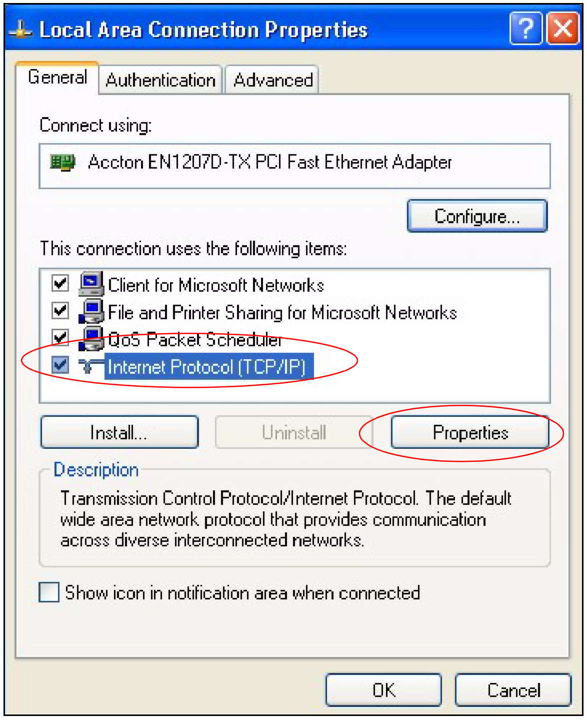
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 200 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 201 Windows XP: Local Area Connection Properties



Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

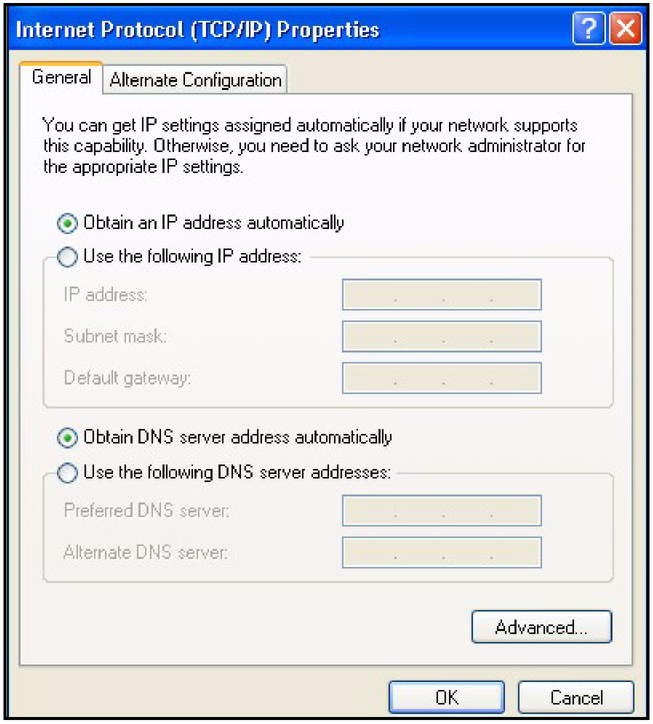
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 202 Windows XP: Internet Protocol (TCP/IP) Properties



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

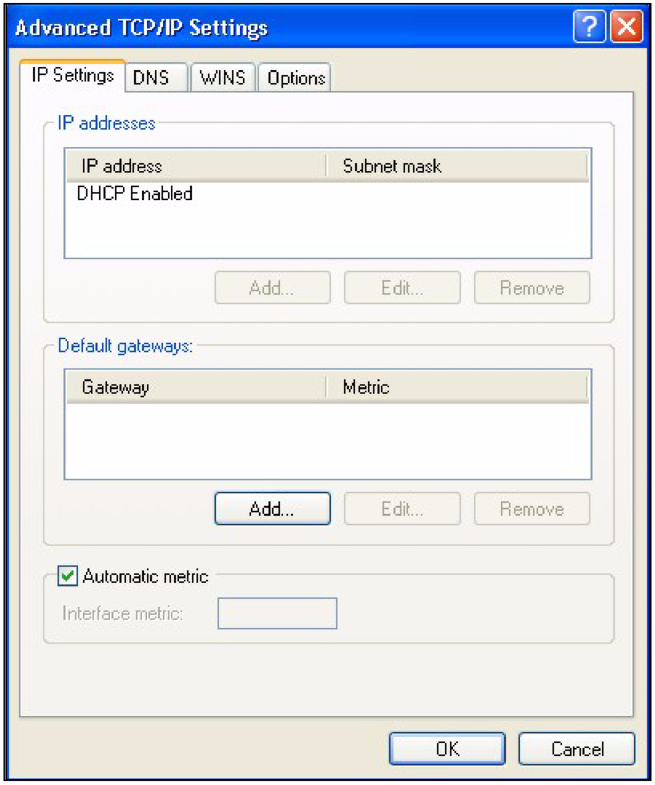
Alternate DNS server:

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 203 Windows XP: Advanced TCP/IP Properties



IP address	Subnet mask
DHCP Enabled	

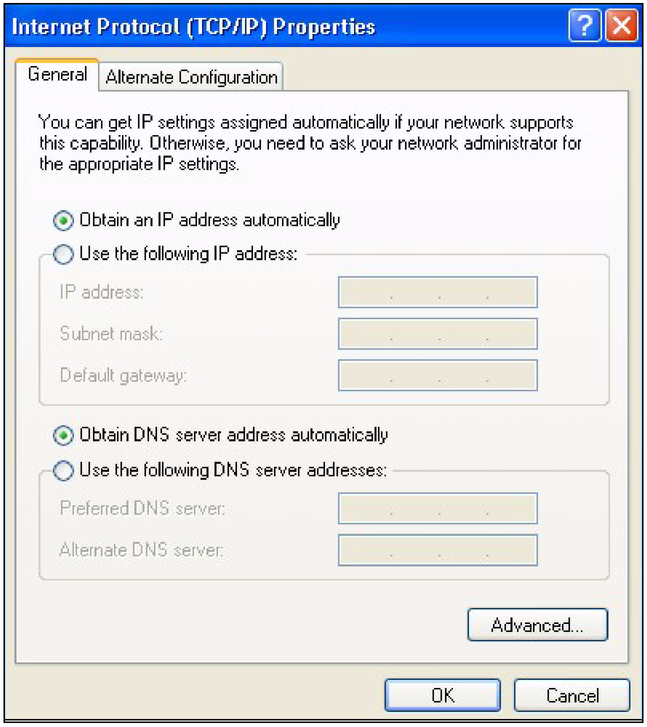
☑ Automatic metric

7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 204 Windows XP: Internet Protocol (TCP/IP) Properties



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

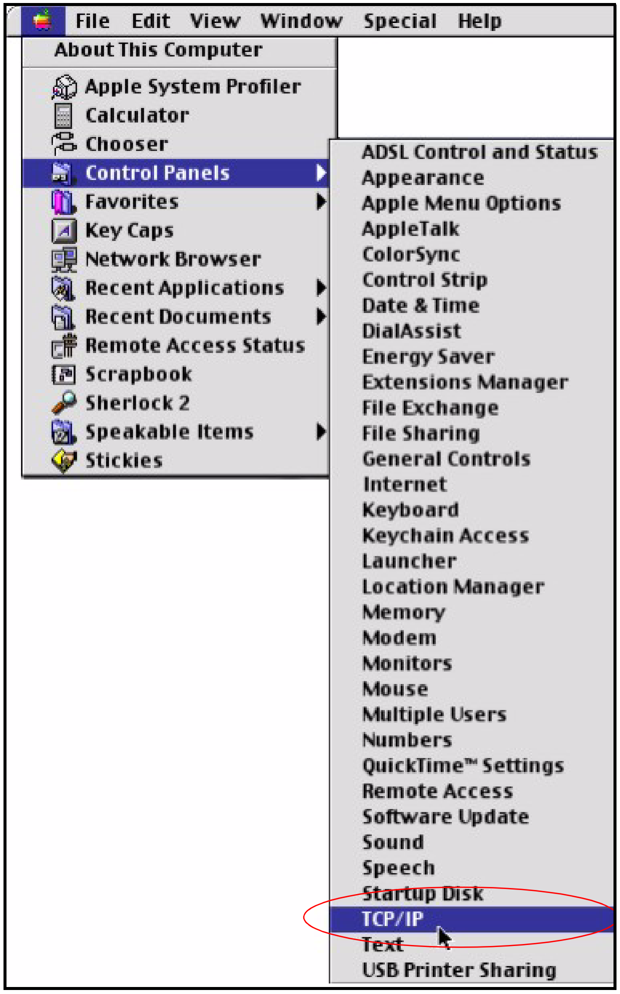
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

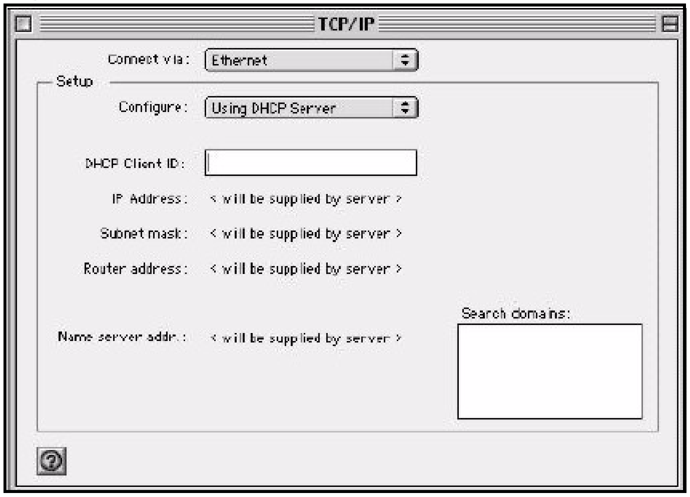
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 205 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 206 Macintosh OS 8/9: TCP/IP


TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

Search domains:

3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.

- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your ZyXEL Device and restart your computer (if prompted).

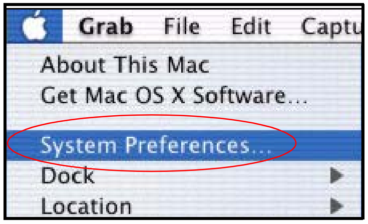
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 207 Macintosh OS X: Apple Menu

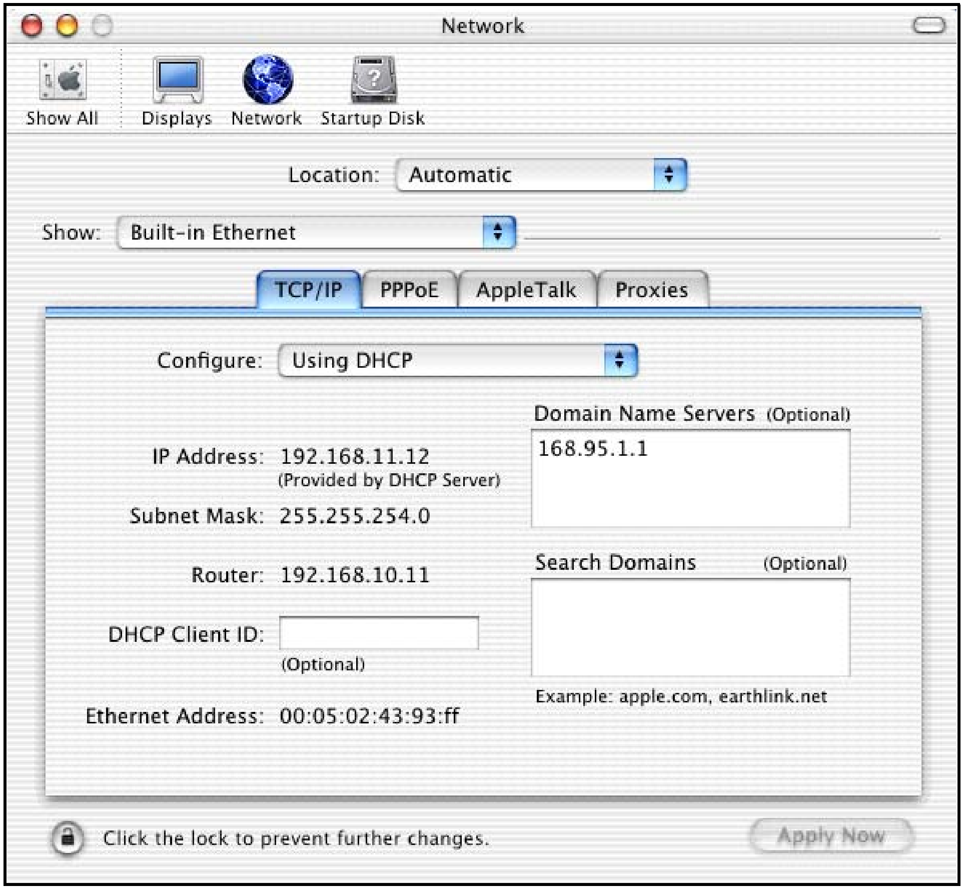


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 208 Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

Domain Name Servers (Optional)

168.95.1.1

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

Search Domains (Optional)

DHCP Client ID:
(Optional)

Example: apple.com, earthlink.net

Ethernet Address: 00:05:02:43:93:ff

4 For statically assigned settings, do the following:
   - From the **Configure** box, select **Manually**.
   - Type your IP address in the **IP Address** box.
   - Type your subnet mask in the **Subnet mask** box.
   - Type the IP address of your ZyXEL Device in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer’s TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

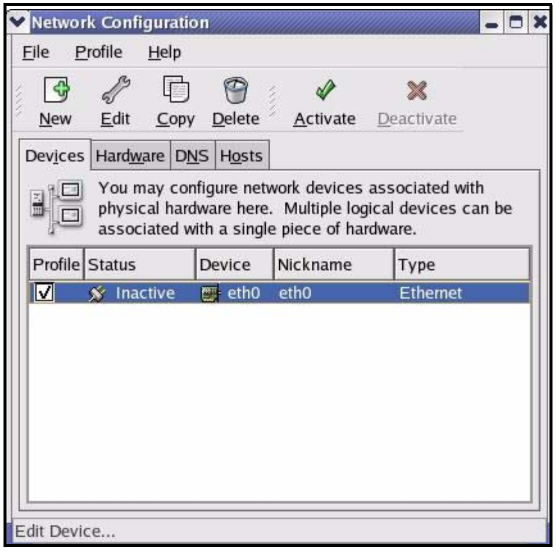
Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 209 Red Hat 9.0: KDE: Network Configuration: Devices

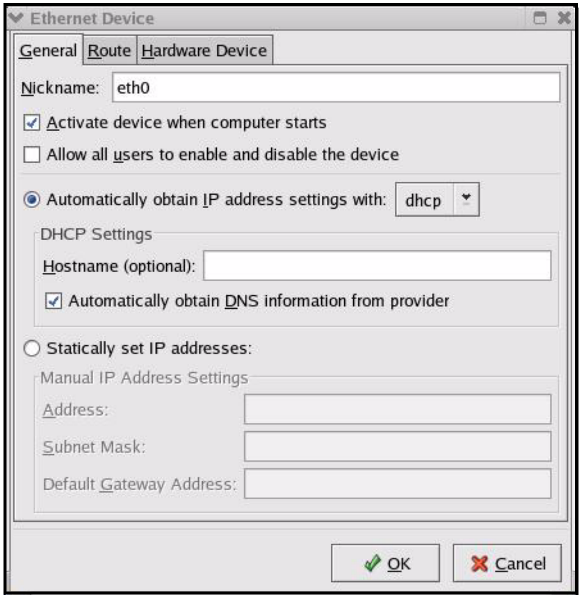


You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

Profile	Status	Device	Nickname	Type
☑	Inactive	eth0	eth0	Ethernet

2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

Figure 210 Red Hat 9.0: KDE: Ethernet Device: General



Nickname: eth0

☑ Activate device when computer starts

☐ Allow all users to enable and disable the device

● Automatically obtain IP address settings with: dhcp

DHCP Settings

Hostname (optional):

☑ Automatically obtain DNS information from provider

○ Statically set IP addresses:

Manual IP Address Settings

Address:

Subnet Mask:

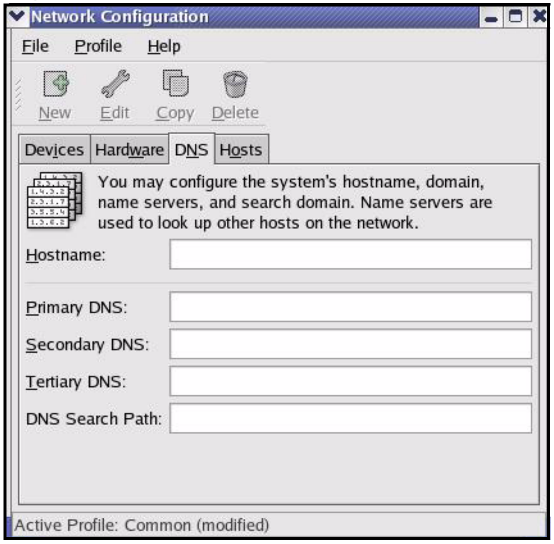
Default Gateway Address:

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 211 Red Hat 9.0: KDE: Network Configuration: DNS



You may configure the system's hostname, domain, name servers, and search domain. Name servers are used to look up other hosts on the network.

Hostname:

Primary DNS:

Secondary DNS:

Tertiary DNS:

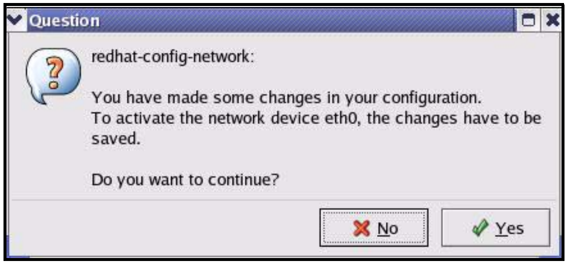
DNS Search Path:

Active Profile: Common (modified)

5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 212 Red Hat 9.0: KDE: Network Configuration: Activate



redhat-config-network:

You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.

Do you want to continue?

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 213 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter `static` in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 214 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 215 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

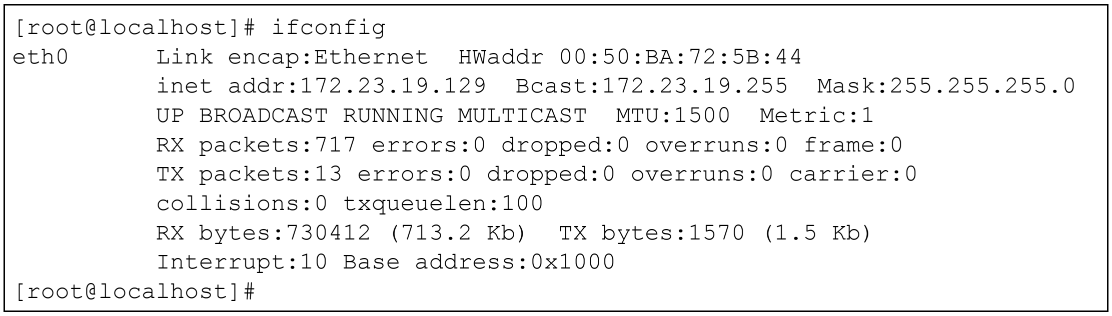
Figure 216 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                      [OK]
Shutting down loopback interface:                  [OK]
Setting network parameters:                        [OK]
Bringing up loopback interface:                    [OK]
Bringing up interface eth0:                        [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 217 Red Hat 9.0: Checking TCP/IP Properties



```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

C

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

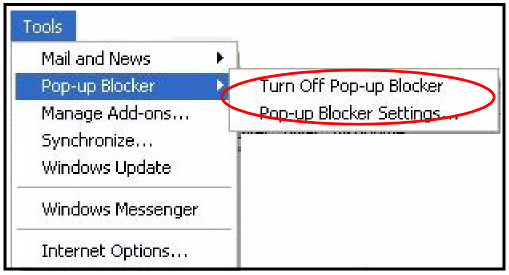
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 218 Pop-up Blocker

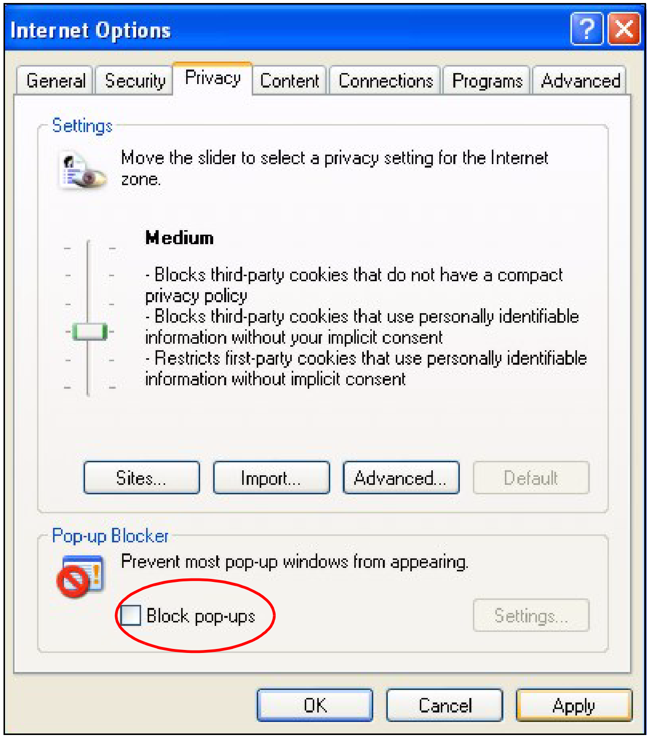


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 219 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

□ Block pop-ups

3 Click **Apply** to save this setting.

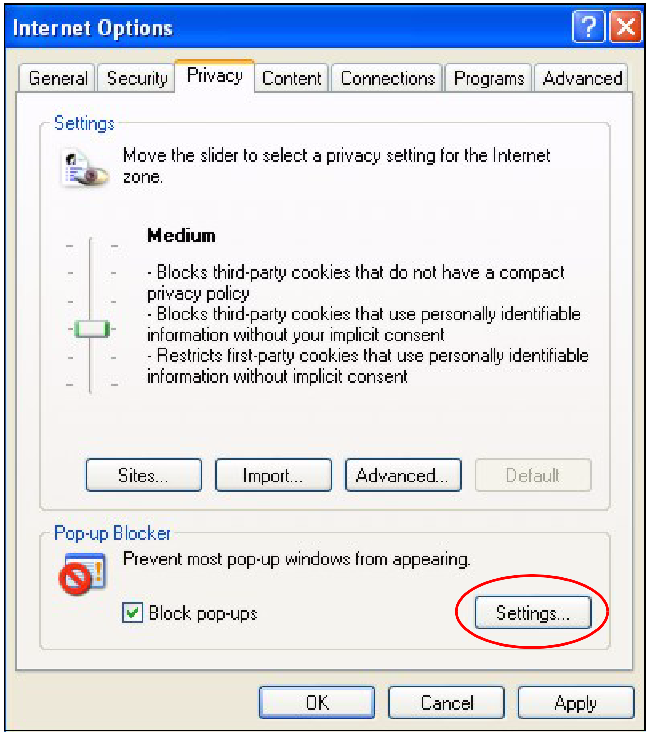
Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 220 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

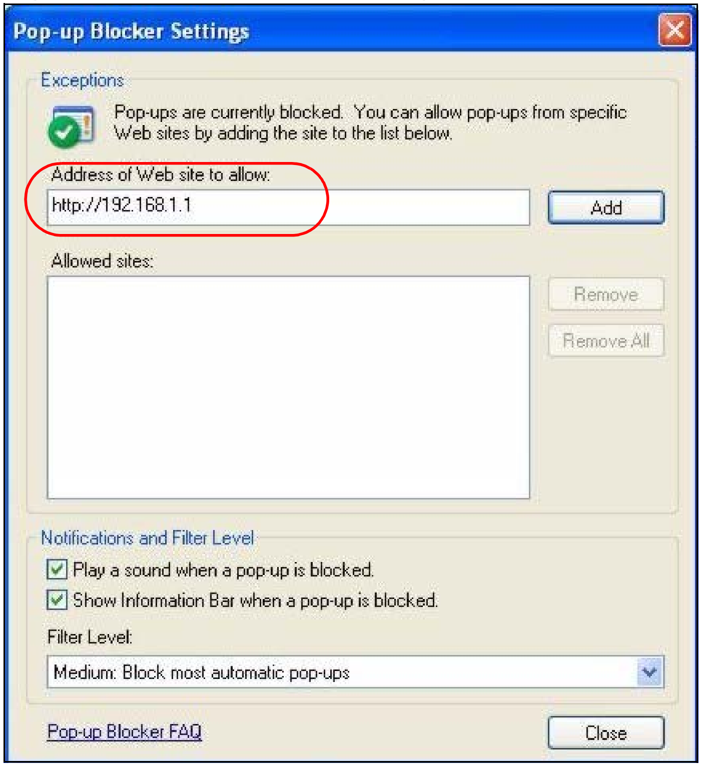
Prevent most pop-up windows from appearing.

☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 221 Pop-up Blocker Settings



Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow: http://192.168.1.1

Allowed sites:

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level: Medium: Block most automatic pop-ups

5 Click **Close** to return to the **Privacy** screen.

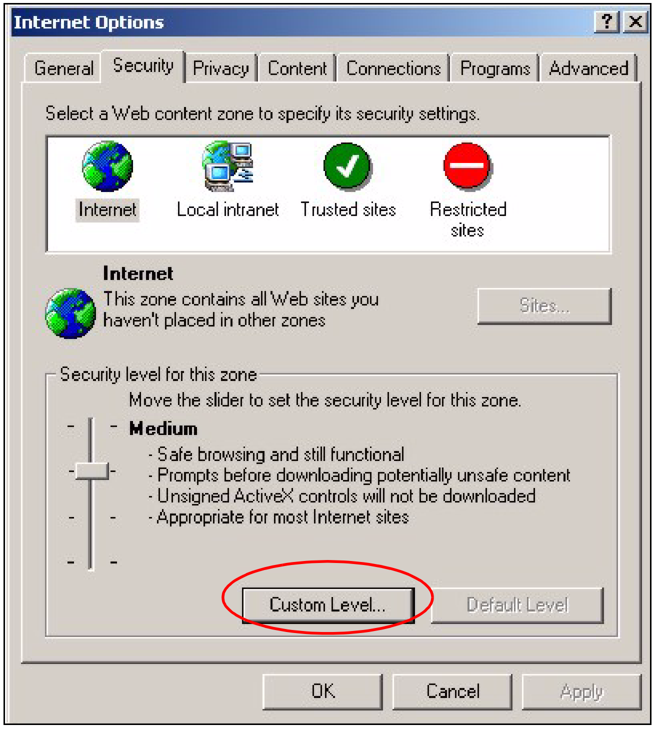
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 222 Internet Options: Security



Select a Web content zone to specify its security settings.

Internet

This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Move the slider to set the security level for this zone.

Medium

- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

2 Click the **Custom Level...** button.

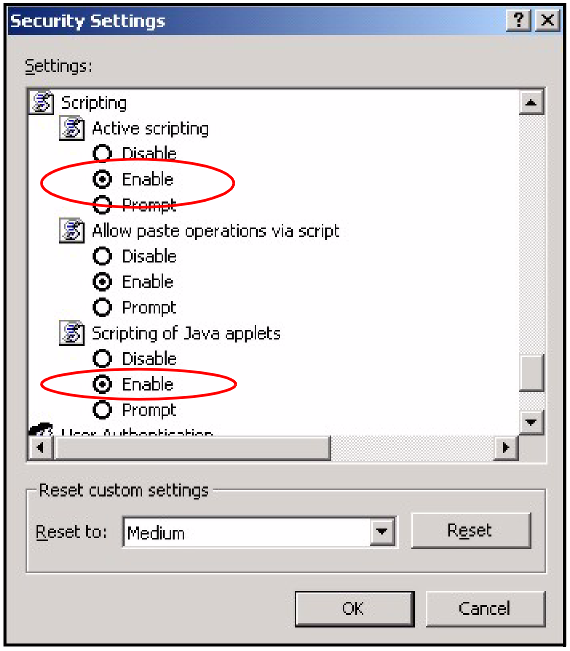
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 223 Security Settings - Java Scripting



Security Settings

Settings:

Scripting
- Active scripting
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Allow paste operations via script
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Scripting of Java applets
  - ○ Disable
  - ● Enable
  - ○ Prompt

User Authentication

Reset custom settings

Reset to: Medium

Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

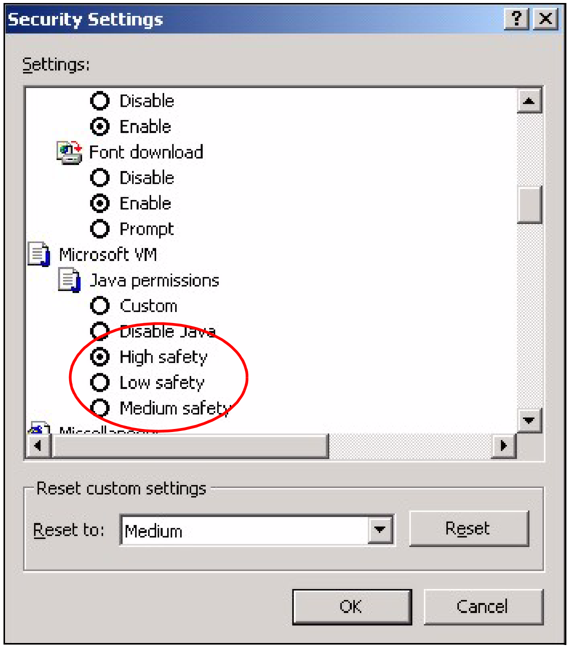
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 224 Security Settings - Java



Security Settings

Settings:

- ○ Disable
- ● Enable

Font download
- ○ Disable
- ● Enable
- ○ Prompt

Microsoft VM
- Java permissions
  - ○ Custom
  - ○ Disable Java
  - ● High safety
  - ○ Low safety
  - ○ Medium safety

Miscellaneous

Reset custom settings

Reset to: Medium

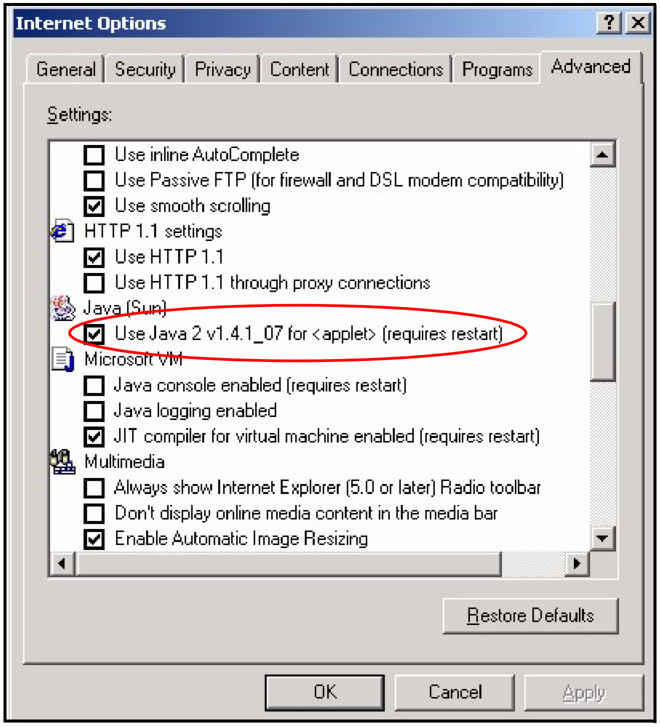
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 225 Java (Sun)



Settings:

□ Use inline AutoComplete
□ Use Passive FTP (for firewall and DSL modem compatibility)
☑ Use smooth scrolling
HTTP 1.1 settings
☑ Use HTTP 1.1
□ Use HTTP 1.1 through proxy connections
Java (Sun)
☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
Microsoft VM
□ Java console enabled (requires restart)
□ Java logging enabled
☑ JIT compiler for virtual machine enabled (requires restart)
Multimedia
□ Always show Internet Explorer (5.0 or later) Radio toolbar
□ Don't display online media content in the media bar
☑ Enable Automatic Image Resizing

D

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

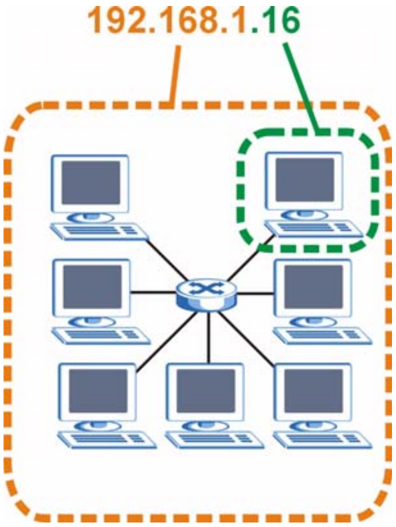
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 226 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 100 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 101 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 102 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} – 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} – 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} – 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} – 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 103 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 103 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

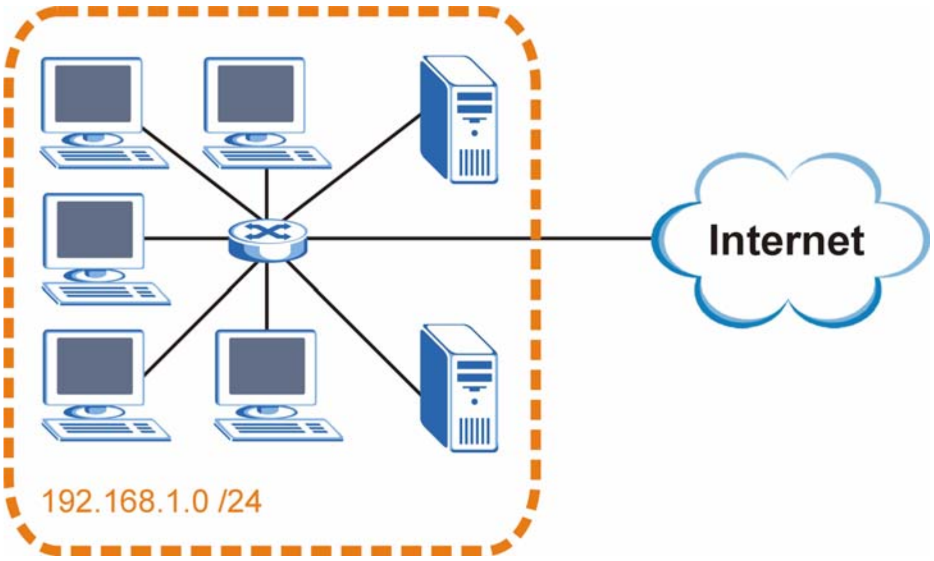
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 – 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 227 Subnetting Example: Before Subnetting

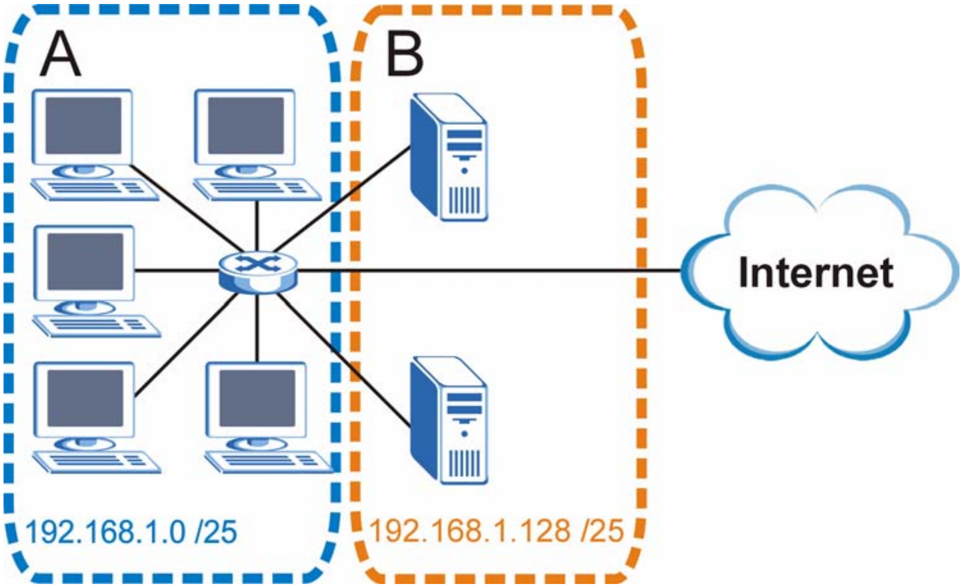


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 228 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 – 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 104 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 105 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 106 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 107 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 108 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 108 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 109 24-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 110 16-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 110 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyXEL Device.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

E

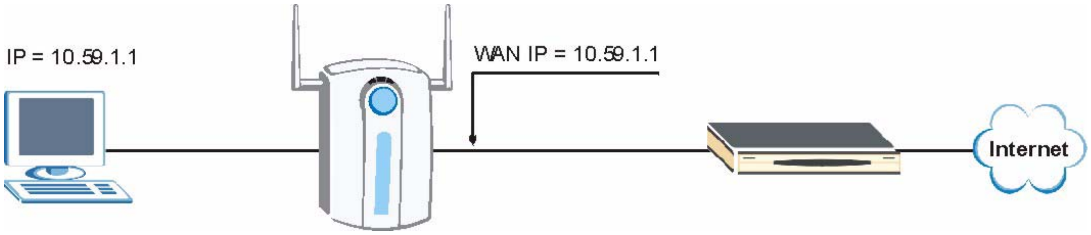
IP Address Assignment Conflicts

This appendix describes situations where IP address conflicts may occur. Subscribers with duplicate IP addresses will not be able to access the Internet.

Case A: The ZyXEL Device is using the same LAN and WAN IP addresses

The following figure shows an example where the ZyXEL Device is using a WAN IP address that is the same as the IP address of a computer on the LAN.

Figure 229 IP Address Conflicts: Case A

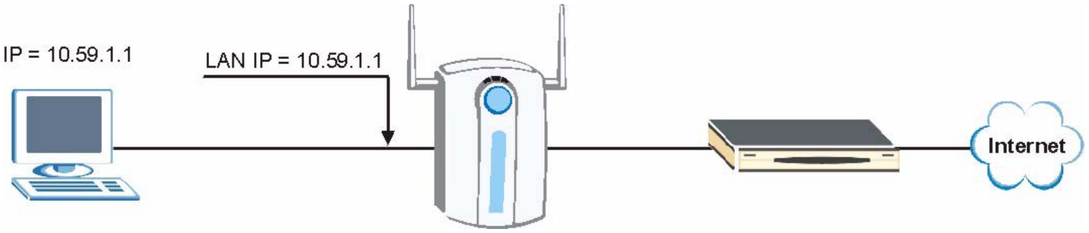


You must set the ZyXEL Device to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the ZyXEL Device. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the ZyXEL Device use a public WAN IP address.

Case B: The ZyXEL Device LAN IP address conflicts with the DHCP client IP address

In the following figure, the ZyXEL Device is acting as a DHCP server. The ZyXEL Device assigns an IP address, which is the same as its LAN port IP address, to a DHCP client attached to the LAN.

Figure 230 IP Address Conflicts: Case B

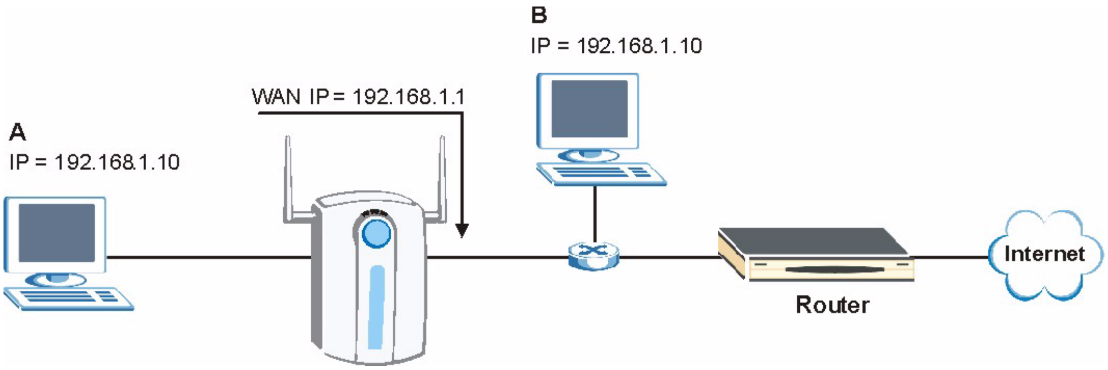


To solve this problem, make sure the ZyXEL Device LAN IP address is not in the DHCP IP address pool.

Case C: The Subscriber IP address is the same as the IP address of a network device

The following figure depicts an example where the subscriber IP address is the same as the IP address of a network device not attached to the ZyXEL Device.

Figure 231 IP Address Conflicts: Case C



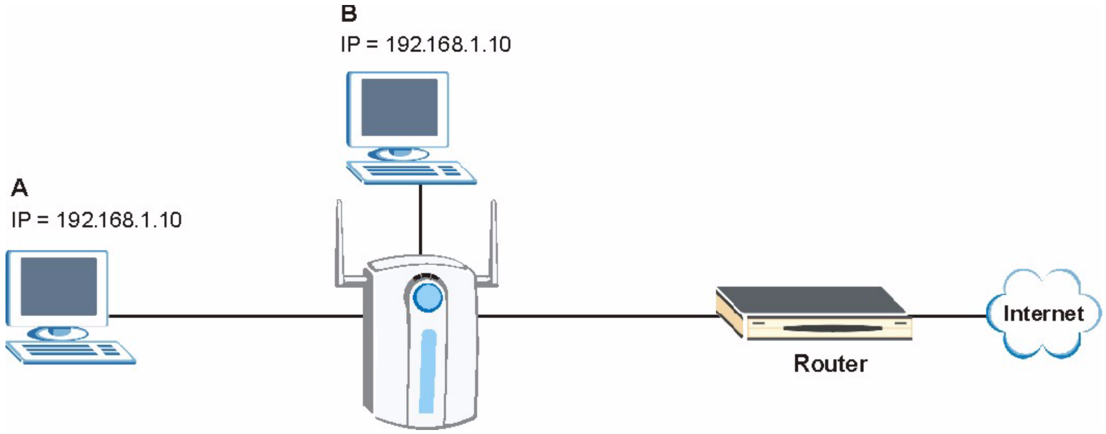
You must set the ZyXEL Device to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the ZyXEL Device. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1. Otherwise, It is recommended the ZyXEL Device uses a public WAN IP address.

Case D: Two or more subscribers have the same IP address.

By converting all private IP addresses to the WAN IP address, the ZyXEL Device allows subscribers with different network configurations to access the Internet. However, there are situations where two or more subscribers are using the same private IP address. This may happen when a subscriber is configured to use a static (or fixed) IP address that is the same as the IP address the ZyXEL Device DHCP server assigns to another subscriber acting as a DHCP client.

In this case, the subscribers are not able to access the Internet.

Figure 232 IP Address Conflicts: Case D



This problem can be solved by adding a VLAN-enabled switch or set the computers to obtain IP addresses dynamically.

F

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 111 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.

Table 111 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.

Table 111 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

G

Command Interpreter

The following describes how to use the command interpreter. See Section 30.1 on page 255 for how to access the command interpreter from SMT. See www.zyxel.com for more detailed information on these commands.

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets <>.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|` symbol means or.

  For example,

  sys filter netbios config <type> <on|off>

  means that you must specify the type of netbios filter and whether to turn it on or off.

Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to close the session when finished.

Command Examples

This section provides some examples of commands you can use on the ZyXEL Device. This list is intended as a general reference of examples. The commands available in your ZyXEL Device may differ from the examples given here. See the other appendices for more examples.

Configuring What You Want the ZyXEL Device to Log

1. Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyXEL Device is to record.
2. Use `sys logs category` to view a list of the log categories.

Figure 233 Displaying Log Categories Example

```
ras> sys logs category
access          display         error           mten
upnp
```

3. Use `sys logs category` followed by a log category to display the parameters that are available for the category.

Figure 234 Displaying Log Parameters Example

```
ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both]
```

4. Use `sys logs category` followed by a log category and a parameter to decide what to record.

   Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. Not every parameter is available with every category.
5. Use the `sys logs save` command to store the settings in the ZyXEL Device (you must do this in order to record logs).

Displaying Logs

- Use the `sys logs display` command to show all of the logs in the ZyXEL Device's log.
- Use the `sys logs category display` command to show the log settings for all of the log categories.
- Use the `sys logs display [log category]` command to show the logs in an individual ZyXEL Device log category.
- Use the `sys logs clear` command to erase all of the ZyXEL Device's logs.

Log Command Example

This example shows how to set the ZyXEL Device to record the access logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category access
ras> sys logs save
ras> sys logs display access
#  .time                 source                 destination            notes

    message
  0|01/01/2000 08:05:03 |192.168.1.33          |207.69.188.186       |ACCESS
OPPED
    NetBIOS packet filtered! source: 0xC0A80121, dest: 0xCF45BCBA
  1|01/01/2000 08:05:03 |192.168.1.33          |207.69.188.186       |ACCESS
OPPED
    NetBIOS packet filtered! source: 0xC0A80121, dest: 0xCF45BCBA
  2|01/01/2000 08:04:57 |192.168.1.33          |207.69.188.186       |ACCESS
OPPED
    NetBIOS packet filtered! source: 0xC0A80121, dest: 0xCF45BCBA
  3|01/01/2000 08:04:57 |192.168.1.33          |207.69.188.186       |ACCESS
OPPED
    NetBIOS packet filtered! source: 0xC0A80121, dest: 0xCF45BCBA
  4|01/01/2000 08:04:53 |192.168.1.33          |207.69.188.186       |ACCESS
OPPED
    NetBIOS packet filtered! source: 0xC0A80121, dest: 0xCF45BCBA
  5|01/01/2000 08:04:53 |192.168.1.33          |207.69.188.186       |ACCESS
OPPED
    NetBIOS packet filtered! source: 0xC0A80121, dest: 0xCF45BCBA
```

Routing Command

Syntax: `ip nat routing [0:LAN] [0:no|1:yes]`

Use this command to set the ZyXEL Device to route traffic that does not match a NAT rule through a specific interface. An example of when you may want to use this is if you have servers with public IP addresses connected to the LAN.

The following command example sets the ZyXEL Device to route traffic that does not match a NAT rule through the LAN interface.

Figure 235   Routing Command Example

```
ras> ip nat routing 2 0
Routing can work in NAT when no NAT rule match.
-----------------------------------------------
         LAN: yes
```

ARP Behavior and the ARP ackGratuitous Commands

The ZyXEL Device does not accept ARP reply information if the ZyXEL Device did not send out a corresponding request. This helps prevent the ZyXEL Device from updating its ARP table with an incorrect IP address to MAC address mapping due to a spoofed ARP. An incorrect IP to MAC address mapping in the ZyXEL Device's ARP table could cause the ZyXEL Device to send packets to the wrong device.

Commands for Using or Ignoring Gratuitous ARP Requests

A host can send an ARP request to resolve its own IP address. This is called a gratuitous ARP request. The packet uses the host's own IP address as the source and destination IP address. The packet uses the Ethernet broadcast address (FF:FF:FF:FF:FF:FF) as the destination MAC address. This is used to determine if any other hosts on the network are using the same IP address as the sending host. The other hosts in the network can also update their ARP table IP address to MAC address mappings with this host's MAC address.

The `ip arp ackGratuitous` commands set how the ZyXEL Device handles gratuitous ARP requests.

- Use `ip arp ackGratuitous active no` to have the ZyXEL Device ignore gratuitous ARP requests.
- Use `ip arp ackGratuitous active yes` to have the ZyXEL Device respond to gratuitous ARP requests.

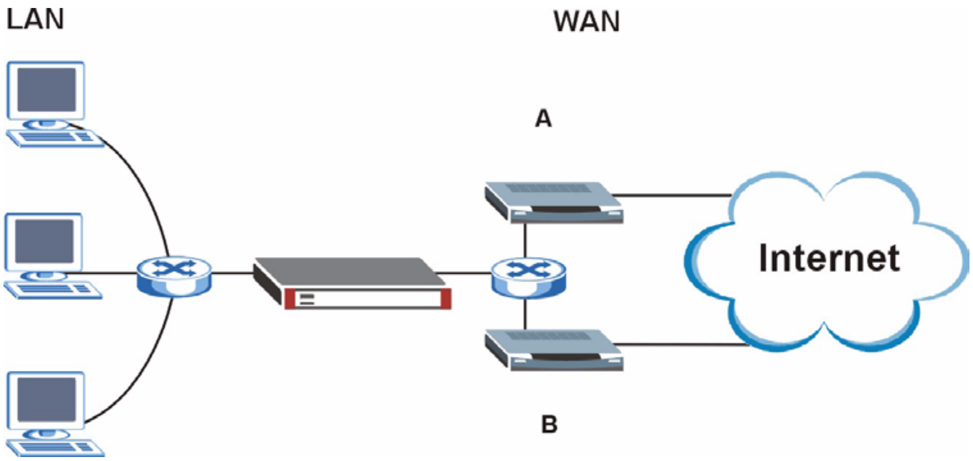
  For example, say the regular gateway goes down and a backup gateway sends a gratuitous ARP request. If the request is for an IP address that is not already in the ZyXEL Device's ARP table, the ZyXEL Device sends an ARP request to ask which host is using the IP address. After the ZyXEL Device receives a reply from the backup gateway, it adds an ARP table entry.

  If the ZyXEL Device's ARP table already has an entry for the IP address, the ZyXEL Device's response depends on how you configure the `ip arp ackGratuitous forceUpdate` command.

  - Use `ip arp ackGratuitous forceUpdate on` to have the ZyXEL Device update the MAC address in the ARP entry.
  - Use `ip arp ackGratuitous forceUpdate off` to have the ZyXEL Device not update the MAC address in the ARP entry.

A backup gateway (as in the following graphic) is an example of when you might want to turn on the forced update for gratuitous ARP requests. One day gateway A shuts down and the backup gateway (B) comes online using the same static IP address as gateway A. Gateway B broadcasts a gratuitous ARP request to ask which host is using its IP address. If ackGratuitous is on and set to force updates, the ZyXEL Device receives the gratuitous ARP request and updates its ARP table. This way the ZyXEL Device has a correct gateway ARP entry to forward packets through the backup gateway. If ackGratuitous is off or not set to force updates, the ZyXEL Device will not update the gateway ARP entry and cannot forward packets through gateway B.

Figure 236 Backup Gateway



Updating the ARP entries could increase the danger of spoofing attacks. It is only recommended that you turn on ackGratuitous and force update if you need it like in the previous backup gateway example. Turning on the force updates option is more dangerous than leaving it off because the ZyXEL Device updates the ARP table even when there is an existing entry.

H

Log Descriptions

This appendix provides descriptions of example log messages.

Table 112 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`WAN interface gets IP:%s`	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns%s`	The DHCP server assigned an IP address to a client.
`Successful WEB login`	Someone has logged on to the router's web configurator interface.
`WEB login failed`	Someone has failed to log on to the router's web configurator interface.
`Successful TELNET login`	Someone has logged on to the router via telnet.
`TELNET login failed`	Someone has failed to log on to the router via telnet.
`Successful FTP login`	Someone has logged on to the router via ftp.
`FTP login failed`	Someone has failed to log on to the router via ftp.
`NAT Session Table is Full!`	The maximum number of NAT session table entries has been exceeded and the table is full.
`Starting Connectivity Monitor`	Starting Connectivity Monitor.
`Time initialized by Daytime Server`	The router got the time and date from the Daytime server.
`Time initialized by Time server`	The router got the time and date from the Time server.
`Time initialized by NTP server`	The router got the time and date from the NTP server.
`Connect to Daytime server fail`	The router was not able to connect to the Daytime server.
`Connect to Time server fail`	The router was not able to connect to the Time server.
`Connect to NTP server fail`	The router was not able to connect to the NTP server.
`Too large ICMP packet has been dropped`	The router dropped an ICMP packet that was too large.
`Configuration Change: PC = 0x%x, Task ID = 0x%x`	The router is saving configuration changes.

Table 112 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
`Successful SSH login`	Someone has logged on to the router’s SSH server.
`SSH login failed`	Someone has failed to log on to the router’s SSH server.
`Successful HTTPS login`	Someone has logged on to the router's web configurator interface using HTTPS protocol.
`HTTPS login failed`	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.

Table 113 System Error Logs

LOG MESSAGE	DESCRIPTION
`%s exceeds the max. number of session per host!`	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
`setNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`readNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`WAN connection is down.`	A WAN connection is down. You cannot access the network through this interface.

Table 114 Access Control Logs

LOG MESSAGE	DESCRIPTION
`Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Router sent blocked web site message: TCP`	The router sent a message to notify a user that the router blocked access to a web site that the user requested.

Table 115 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
`Under SYN flood attack, sent TCP RST`	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
`Exceed TCP MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.)
`Peer TCP state out of order, sent TCP RST`	The router sent a TCP reset packet when a TCP connection state was out of order.

Table 116 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
`[TCP | UDP | ICMP | IGMP | Generic] packet filter matched (set:%d, rule:%d)`	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

Table 117 ICMP Logs

LOG MESSAGE	DESCRIPTION
`Packet without a NAT table entry blocked: ICMP`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Router reply ICMP packet: ICMP`	The router sent an ICMP reply packet to the sender.

Table 118 CDR Logs

LOG MESSAGE	DESCRIPTION
`board%d line%d channel%d, call%d,%s C01 Outgoing Call dev=%x ch=%x%s`	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or "ch" is the call channel ID.For example,"board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times.
`board%d line%d channel%d, call%d,%s C02 OutCall Connected%d%s`	The PPPoE, PPTP or dial-up call is connected.
`board%d line%d channel%d, call%d,%s C02 Call Terminated`	The PPPoE, PPTP or dial-up call was disconnected.

Table 119 PPP Logs

LOG MESSAGE	DESCRIPTION
`ppp:LCP Starting`	The PPP connection's Link Control Protocol stage has started.
`ppp:LCP Opening`	The PPP connection's Link Control Protocol stage is opening.
`ppp:CHAP Opening`	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
`ppp:IPCP Starting`	The PPP connection's Internet Protocol Control Protocol stage is starting.
`ppp:IPCP Opening`	The PPP connection's Internet Protocol Control Protocol stage is opening.
`ppp:LCP Closing`	The PPP connection's Link Control Protocol stage is closing.
`ppp:IPCP Closing`	The PPP connection's Internet Protocol Control Protocol stage is closing.

Table 120 IKE Logs

LOG MESSAGE	DESCRIPTION
`Active connection allowed exceeded`	The IKE process for a new connection failed because the limit of simultaneous phase 2 SAs has been reached.
`Start Phase 2: Quick Mode`	Phase 2 Quick Mode has started.
`Verifying Remote ID failed:`	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
`Verifying Local ID failed:`	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.

Table 120 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`IKE Packet Retransmit`	The router retransmitted the last packet sent because there was no response from the peer.
`Failed to send IKE Packet`	An Ethernet error stopped the router from sending IKE packets.
`Too many errors! Deleting SA`	An SA was deleted because there were too many errors.
`Phase 1 IKE SA process done`	The phase 1 IKE SA process has been completed.
`Duplicate requests with the same cookie`	The router received multiple requests from the same peer while still processing the first IKE packet from the peer.
`IKE Negotiation is in process`	The router has already started negotiating with the peer for the connection, but the IKE process has not finished yet.
`No proposal chosen`	Phase 1 or phase 2 parameters don't match. Please check all protocols / settings. Ex. One device being configured for 3DES and the other being configured for DES causes the connection to fail.
`Local / remote IPs of incoming request conflict with rule <%d>`	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
`Cannot resolve Secure Gateway Addr for rule <%d>`	The router couldn't resolve the IP address from the domain name that was used for the secure gateway address.
`Peer ID: <peer id> <My remote type> -<My local type>`	The displayed ID information did not match between the two ends of the connection.
`vs. My Remote <My remote> - <My remote>`	The displayed ID information did not match between the two ends of the connection.
`vs. My Local <My local>-<My local>`	The displayed ID information did not match between the two ends of the connection.
`Send <packet>`	A packet was sent.
`Recv <packet>`	IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the LOG. Refer to RFC2408 – ISAKMP for a list of all ISAKMP payload types.
`Recv <Main or Aggressive> Mode request from <IP>`	The router received an IKE negotiation request from the peer address specified.
`Send <Main or Aggressive> Mode request to <IP>`	The router started negotiation with the peer.
`Invalid IP <Peer local> / <Peer local>`	The peer's "Local IP Address" is invalid.
`Remote IP <Remote IP> / <Remote IP> conflicts`	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
`Phase 1 ID type mismatch`	This router's "Peer ID Type" is different from the peer IPSec router's "Local ID Type".
`Phase 1 ID content mismatch`	This router's "Peer ID Content" is different from the peer IPSec router's "Local ID Content".
`No known phase 1 ID type found`	The router could not find a known phase 1 ID in the connection attempt.

Table 120 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`ID type mismatch. Local / Peer: <Local ID type/Peer ID type>`	The phase 1 ID types do not match.
`ID content mismatch`	The phase 1 ID contents do not match.
`Configured Peer ID Content: <Configured Peer ID Content>`	The phase 1 ID contents do not match and the configured "Peer ID Content" is displayed.
`Incoming ID Content: <Incoming Peer ID Content>`	The phase 1 ID contents do not match and the incoming packet's ID content is displayed.
`Unsupported local ID Type: <%d>`	The phase 1 ID type is not supported by the router.
`Build Phase 1 ID`	The router has started to build the phase 1 ID.
`Adjust TCP MSS to%d`	The router automatically changed the TCP Maximum Segment Size value after establishing a tunnel.
`Rule <%d> input idle time out, disconnect`	The tunnel for the listed rule was dropped because there was no inbound traffic within the idle timeout period.
`XAUTH succeed! Username: <Username>`	The router used extended authentication to authenticate the listed username.
`XAUTH fail! Username: <Username>`	The router was not able to use extended authentication to authenticate the listed username.
`Rule[%d] Phase 1 negotiation mode mismatch`	The listed rule’s IKE phase 1 negotiation mode did not match between the router and the peer.
`Rule [%d] Phase 1 encryption algorithm mismatch`	The listed rule’s IKE phase 1 encryption algorithm did not match between the router and the peer.
`Rule [%d] Phase 1 authentication algorithm mismatch`	The listed rule’s IKE phase 1 authentication algorithm did not match between the router and the peer.
`Rule [%d] Phase 1 authentication method mismatch`	The listed rule’s IKE phase 1 authentication method did not match between the router and the peer.
`Rule [%d] Phase 1 key group mismatch`	The listed rule’s IKE phase 1 key group did not match between the router and the peer.
`Rule [%d] Phase 2 protocol mismatch`	The listed rule’s IKE phase 2 protocol did not match between the router and the peer.
`Rule [%d] Phase 2 encryption algorithm mismatch`	The listed rule’s IKE phase 2 encryption algorithm did not match between the router and the peer.
`Rule [%d] Phase 2 authentication algorithm mismatch`	The listed rule’s IKE phase 2 authentication algorithm did not match between the router and the peer.
`Rule [%d] Phase 2 encapsulation mismatch`	The listed rule’s IKE phase 2 encapsulation did not match between the router and the peer.
`Rule [%d]> Phase 2 pfs mismatch`	The listed rule’s IKE phase 2 perfect forward secret (pfs) setting did not match between the router and the peer.
`Rule [%d] Phase 1 ID mismatch`	The listed rule’s IKE phase 1 ID did not match between the router and the peer.
`Rule [%d] Phase 1 hash mismatch`	The listed rule’s IKE phase 1 hash did not match between the router and the peer.

Table 120 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`Rule [%d] Phase 1 preshared key mismatch`	The listed rule’s IKE phase 1 pre-shared key did not match between the router and the peer.
`Rule [%d] Tunnel built successfully`	The listed rule’s IPSec tunnel has been built successfully.
`Rule [%d] Peer's public key not found`	The listed rule’s IKE phase 1 peer’s public key was not found.
`Rule [%d] Verify peer's signature failed`	The listed rule’s IKE phase 1verification of the peer’s signature failed.
`Rule [%d] Sending IKE request`	IKE sent an IKE request for the listed rule.
`Rule [%d] Receiving IKE request`	IKE received an IKE request for the listed rule.
`Swap rule to rule [%d]`	The router changed to using the listed rule.
`Rule [%d] Phase 1 key length mismatch`	The listed rule’s IKE phase 1 key length (with the AES encryption algorithm) did not match between the router and the peer.
`Rule [%d] phase 1 mismatch`	The listed rule’s IKE phase 1 did not match between the router and the peer.
`Rule [%d] phase 2 mismatch`	The listed rule’s IKE phase 2 did not match between the router and the peer.
`Rule [%d] Phase 2 key length mismatch`	The listed rule’s IKE phase 2 key lengths (with the AES encryption algorithm) did not match between the router and the peer.

Table 121 PKI Logs

LOG MESSAGE	DESCRIPTION
`Enrollment successful`	The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port.
`Enrollment failed`	The SCEP online certificate enrollment failed. The Destination field records the certification authority server’s IP address and port.
`Failed to resolve <SCEP CA server url>`	The SCEP online certificate enrollment failed because the certification authority server’s address cannot be resolved.
`Enrollment successful`	The CMP online certificate enrollment was successful. The Destination field records the certification authority server’s IP address and port.
`Enrollment failed`	The CMP online certificate enrollment failed. The Destination field records the certification authority server’s IP address and port.
`Failed to resolve <CMP CA server url>`	The CMP online certificate enrollment failed because the certification authority server’s IP address cannot be resolved.
`Rcvd ca cert: <subject name>`	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd user cert: <subject name>`	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.

Table 121 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
`Rcvd CRL <size>: <issuer name>`	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd ARL <size>: <issuer name>`	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ca cert`	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received user cert`	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received CRL`	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ARL`	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Rcvd data <size> too large! Max size allowed: <max size>`	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
`Cert trusted: <subject name>`	The router has verified the path of the certificate with the listed subject name.
`Due to <reason codes>, cert not trusted: <subject name>`	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 122 on page 337 for the corresponding descriptions of the codes.

Table 122 Certificate Path Verification Failure Reason Codes

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)

Table 122 Certificate Path Verification Failure Reason Codes (continued)

CODE	DESCRIPTION
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 123 ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(L to L)	LAN to LAN/ ZyXEL Device	ACL set for packets traveling from the LAN to the LAN or the ZyXEL Device.
(W to W)	WAN to WAN/ ZyXEL Device	ACL set for packets traveling from the WAN to the WAN or the ZyXEL Device.

Table 124 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench

Table 124 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 125 Syslog Logs

LOG MESSAGE	DESCRIPTION
`<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>`	"This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU->LOGS->Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 126 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal

Table 126 RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Log Commands

This section provides some general examples of how to use the log commands. The items that display with your device may vary but the basic function should be the same.

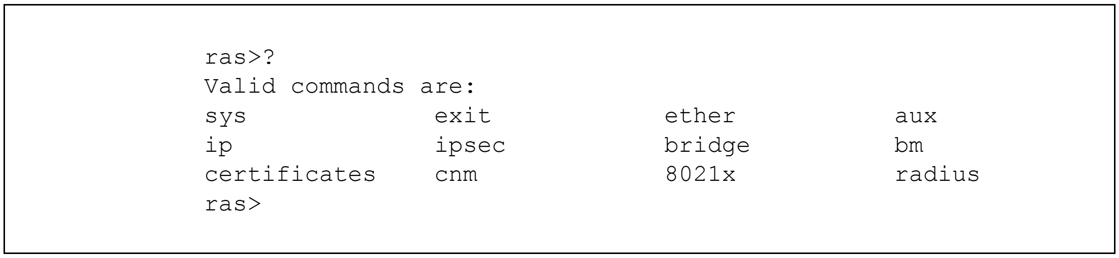
Go to the command interpreter interface. Appendix G on page 325 explains how to access and use the commands.

Configuring What You Want the ZyXEL Device to Log

1 Use the sys logs load command to load the log setting buffer that allows you to configure which logs the ZyXEL Device is to record.

2 Use sys logs category to view a list of the log categories.

Figure 237 Displaying Log Categories Example



```
ras>?
Valid commands are:
sys             exit            ether           aux
ip              ipsec           bridge          bm
certificates    cnm             8021x           radius
ras>
```

3 Use sys logs category followed by a log category to display the parameters that are available for the category.

Figure 238 Displaying Log Parameters Example

```
ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both]
```

4 Use sys logs category followed by a log category and a parameter to decide what to record.

Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. Not every parameter is available with every category.

5 Step 5.Use the sys logs save command to store the settings in the ZyXEL Device (you must do this in order to record logs).

Displaying Logs

- Use the sys logs display command to show all of the logs in the ZyXEL Device's log.
- Use the sys logs category display command to show the log settings for all of the log categories.
- Use the sys logs display [log category] command to show the logs in an individual ZyXEL Device log category.
- Use the sys logs clear command to erase all of the ZyXEL Device's logs.

I

NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands. See Appendix G on page 325 for information on the command structure.

Introduction

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.

For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.

You can configure NetBIOS filters to do the following:

- Allow or disallow the sending of NetBIOS packets from the LAN to the WAN and from the WAN to the LAN.
- Allow or disallow NetBIOS packets to initiate calls.

Display NetBIOS Filter Settings

Syntax: `sys filter netbios disp`

This command gives a read-only list of the current NetBIOS filter modes for The ZyXEL Device.

NetBIOS Display Filter Settings Command Example

```
=========== NetBIOS Filter Status ===========
        Between LAN and WAN: Block
              IPSec Packets: Forward
        Trigger Dial: Disabled
```

The filter types and their default settings are as follows.

Table 127 NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
Between LAN and WAN	This field displays whether NetBIOS packets are blocked or forwarded between the LAN and the WAN.	Block
Trigger dial	This field displays whether NetBIOS packets are allowed to initiate calls. Disabled means that NetBIOS packets are blocked from initiating calls.	Disabled

NetBIOS Filter Configuration

```
Syntax:sys filter netbios config <type> <on|off>
```

where

`<type> =` Identify which NetBIOS filter (numbered 0-3) to configure.

0 = Between LAN and WAN

3 = IPSec packet pass through

4 = Trigger Dial

`<on|off> =` For type 0 and 1, use on to enable the filter and block NetBIOS packets. Use off to disable the filter and forward NetBIOS packets.

For type 4, use on to allow NetBIOS packets to initiate dial backup calls. Use off to block NetBIOS packets from initiating dial backup calls.

Example commands

`sys filter netbios config 0 on` This command blocks LAN to WAN and WAN to LAN NetBIOS packets.

`sys filter netbios config 3 on` This command blocks IPSec NetBIOS packets.

`sys filter netbios config 4 off` This command stops NetBIOS commands from initiating calls.

J

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications (Class B)

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of

ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

S

Customer Support

Please have the following information ready when you contact customer support.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- FTP: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz

- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.us.zyxel.com
- FTP: ftp.us.zyxel.com

- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5^{a} planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index